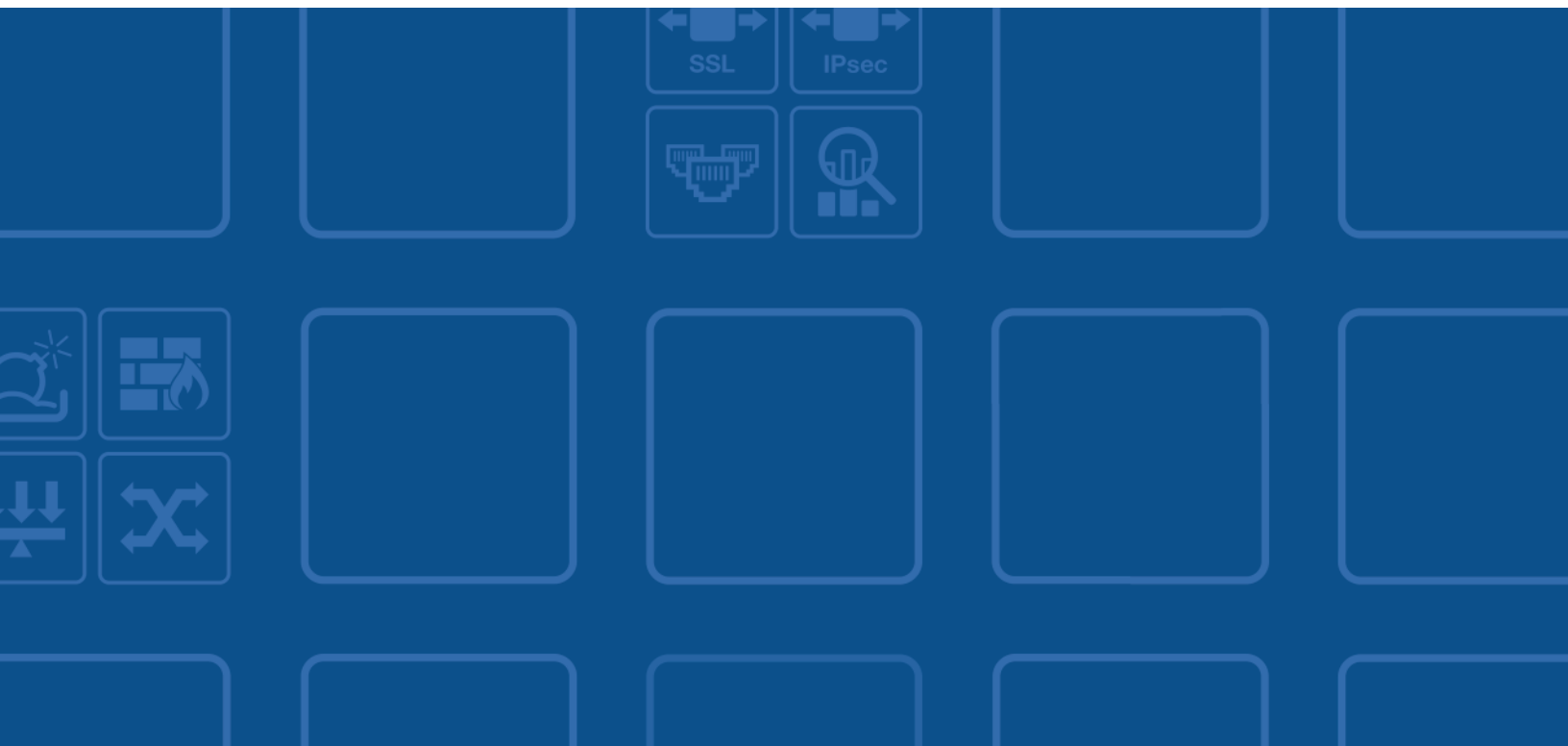
FortiManager - Administration Guide

VERSION 5.4.5



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

February 14, 2018

FortiManager 5.4.5 Administration Guide

02-545-309869-20180214

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-02-14	Initial release of 5.4.5.

Introduction

FortiManager Security Management appliances allow you to centrally manage any number of Fortinet Network Security devices, from several to thousands, including FortiGate, FortiWiFi, and FortiAP devices. Network administrators can better control their network by logically grouping devices into administrative domains (ADOMs), efficiently applying policies and distributing content security/firmware updates. FortiManager is one of several versatile Network Security Management Products that provide a diversity of deployment types, growth flexibility, advanced customization through APIs and simple licensing.

FortiManager features

FortiManager provides the following features:

- Provides easy centralized configuration, policy-based provisioning, update management and end-to-end network monitoring for your Fortinet installation,
- Segregate management of large deployments easily and securely by grouping devices and agents into geographic or functional ADOMs,
- Reduce your management burden and operational costs with fast device and agent provisioning, detailed revision tracking, and thorough auditing capabilities,
- Easily manage complex mesh and star VPN environments while leveraging FortiManager as a local distribution point for software and policy updates,
- Seamless integration with FortiAnalyzer appliances provides in-depth discovery, analysis, prioritization and reporting of network security events,
- Quickly create and modify policies/objects with a consolidated, drag and drop enabled, in-view editor,
- Script and automate device provisioning, policy pushing, etc. with JSON APIs or build custom web portals with the XML API,
- Leverage powerful device profiles for mass provisioning and configuration of managed devices,
- Centrally control firmware upgrades and content security updates from FortiGuard Center Threat Research & Response,
- Deploy with either a physical hardware appliance or virtual machine with multiple options to dynamically increase storage

FortiManager system architecture emphasizes reliability, scalability, ease of use, and easy integration with third-party systems.

FortiManager feature set

The FortiManager feature set includes the following modules:

- Device Manager
- Policy & Objects
- AP Manager
- FortiClient Manager
- VPN Manager
- FortiGuard
- System Settings

FortiAnalyzer feature set

The FortiAnalyzer feature set can be enabled in FortiManager. The FortiAnalyzer feature set includes the following panes:

- FortiView
- Log View
- Event Monitor
- Reports

For information on using the FortiAnalyzer feature set, see the *FortiAnalyzer Administration Guide*.

The FortiAnalyzer feature set is disabled by default. To enable the features, turn it on from the dashboard (see System Information widget on page 327), 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
```

About this document

This document describes how to configure and manage your FortiManager system and the devices that it manages.

The FortiManager documentation assumes that you have one or more FortiGate units and documentation for the FortiGate unit. It also assumes that you are familiar with configuring your FortiGate units before using the FortiManager system. Where FortiManager system features or parts of features are identical to the FortiGate unit's, the FortiManager system documentation refers to the FortiGate unit documentation for further configuration assistance with that feature.

FortiManager documentation

The following FortiManager product documentation is available:

- *FortiManager Administration Guide*
  This document describes how to set up the FortiManager system and use it to manage supported Fortinet units. It includes information on how to configure multiple Fortinet units, configuring and managing the FortiGate VPN policies, monitoring the status of the managed devices, viewing and analyzing the FortiGate logs, updating the virus and attack signatures, providing web filtering and email filter service to the licensed FortiGate units as a local FortiGuard Distribution Server (FDS), firmware revision control and updating the firmware images of the managed units.
- *FortiManager device QuickStart Guides*
  These documents are included with your FortiManager system package. Use these document to install and begin working with the FortiManager system and FortiManager Graphical User Interface (GUI).
- *FortiManager Online Help*
  You can get online help from the FortiManager GUI. FortiManager online help contains detailed procedures for using the FortiManager GUI to configure and manage FortiGate units.
- *FortiManager CLI Reference*
  This document describes how to use the FortiManager Command Line Interface (CLI) and contains references for all FortiManager CLI commands.
- *FortiManager Release Notes*
  This document describes new features and enhancements in the FortiManager system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.
- *FortiManager VM Install Guide*
  This document describes installing FortiManager VM in your virtual environment.

What's New

FortiManager version 5.4 includes the following new features and enhancements. Always review all sections in the *FortiManager Release Notes* prior to upgrading your device.

Not all features/enhancements listed below are supported on all models.

FortiManager version 5.4.5

FortiManager version 5.4.5 includes no new features.

FortiManager version 5.4.4

FortiManager version 5.4.4 includes the following new features and enhancements:

- The Policy Packages and Object Configurations tabs can now be viewed on a single pane. See Display options on page 191 for details.

FortiManager version 5.4.3

FortiManager version 5.4.3 includes the following new features and enhancements:

FortiMeter update

FortiOS VM resourced based metering is now available. The license model is based on the CPU and memory usage. In this update, more granular service offerings, such as FW+1 Service, FW+2 Services, FW+3 Services, and FW +UTM, are provided. It supports up to four interfaces and two VDOMs.

FortiWebOS-VM traffic volume and traffic consumption based metering is also available.

For more information, see FortiMeter on page 178.

Central DNAT per policy package support

DNAT policies can be created on the Central DNAT page of a policy package by creating a new virtual IP (VIP) or importing an existing VIP. The newly created VIP object from the DNAT policy is saved to both the VIP object table from which it can be used by different policy packages in that ADOM.

For more information, see Central DNAT on page 220.

FortiManager version 5.4.2

FortiManager version 5.4.2 includes the following new features and enhancements:

Policy Search and Filtering

The *Column Filter* option is now available from the *Search* box. You add filters from the search box or from the contextual menu by right-clicking an object entry. See Policy search and filter on page 202.

Admin Profile Granularity

Additional options are available to help granular control of administrative access privileges. The new options include:

- Licensing, Firmware Management and Advanced for FortiGuard Center
- Revert Configuration from Revision History for Device Manager
- Interface Mapping for Policy & Objects

See Administrator profiles on page 78.

Automatically Promote Device with Pre-shared Key

Automatically promote a model device to a managed device by using a pre-shared secret.

First you 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 <FMGSN> <KEY>` command from the FortiGate's console. The device is now automatically promoted, and the configuration of the matched model device is applied. See Add a model device on page 100.

For FortiOS 5.4.1 or earlier, you must run the `execute central-mgmt register-device <FMGSN> <KEY> <username> <password>` command.

Package Management Usability

Improved the information display for FortiGuard Package Management. See Package management on page 318.

FortiManager version 5.4.1

FortiManager version 5.4.1 includes the following new features and enhancements:

FortiAP Management

Central Profiles and Monitoring

Improved organization of large AP environments, which includes a simplified workflow and layout of settings and monitored statistics. The full AP health dashboard is now available inside the FortiManager AP Manager component. See Quick status bar on page 262.

Google Map Support

Google map support for location management of APs. See Map View on page 274.

AP Groups

Ability to organize all APs into groups for applying common configuration profiles or monitoring templates. See FortiAP groups on page 267.

Provisioning

Automatically Promote Model Device

Support for zero-touch on-site FortiGate deployment by automatically promoting a model device to a managed device. First you add the model device to FortiManager by using the serial number. Later when the device with that serial number connects to FortiManager, the device is automatically promoted and a configuration applied. See Add a model device on page 100.

VPN Manager

New Wizard

A new VPN wizard is available to help you easily provision and configure VPNs. The new wizard includes all of the previous wizard functions, plus certificate-based deployments, in a more user friendly (graphical) format. See:

- VPN Topology Setup Wizard—see Create IPsec VPN communities on page 243
- VPN Gateway Setup Wizard—see Create a VPN managed gateway on page 250

Migration

Backup and Restore Between Models

Ability to restore the database backup file from one platform to a different platform. See Migrating the configuration on page 332.

Upgrade

One-Step ADOM Upgrade to 5.4

One-step migration procedure to convert a 5.2-based ADOM to a 5.4-based ADOM. See ADOM versions on page 50.

Secure DNS Server

Support for running FortiGuard Secure DNS service on FortiManager. Enabling FortiManager Secure DNS service requires installing a dedicated software build and a license. For information, see the *FortiManager Secure DNS Guide*.

VM Support

Microsoft Azure Cloud

FortiManager/FortiAnalyzer VM is now available from Azure Cloud. See the *FortiManager 5.4 VM Install Guide* for more details.

GUI Themes Support

Multiple color themes are now available for the FortiManager GUI. See Configuring global administrative settings on page 88.

CLI

This section highlights new command line interface (CLI) commands. For more information, see the *FortiManager CLI Reference*.

Global import

After you import an object from a device database to an ADOM database, use the new execute `fmpolicy promote-adom-object` command to import the object into the global database. The object can then be used in global policy packages that can be assigned to multiple ADOMs.

Model migration

You can now move a FortiManager configuration from one model to another using the new `execute migrate all-settings` command. System Settings are not migrated. See Migrating the configuration on page 332.

FortiManager version 5.4.0

FortiManager version 5.4.0 includes the following new features and enhancements:

New GUI look

The FortiManager GUI has a new look and simplified navigation. When ADOMs are enabled, you can now select an ADOM when you log into FortiManager. After you log in, you can choose which pane to display by choosing one of the following options:

- *Device Manager*
- *Policy & Objects*
- *AP Manager*
- *FortiClient Manager*
- *VPN Manager*
- *FortiGuard*
- *System Settings*

When FortiAnalyzer features are enabled, you can also access the following panes: *FortiView*, *Log View*, *Event Monitor*, and *Reports*. See GUI overview on page 34.

Device Manager improvements

The *Device Manager* pane offers several improvements:

- Quick device status: You can now use the quick status bar at the top of the *Device Manager* pane to quickly view the number of devices in a group and how many devices in the group have modified configurations, modified policy packages, or connection problems. You can also click the quick status bar to filter the *Device Manager* pane to display only the devices with modified configurations, modified policy packages, or connection problems. See Using the quick status bar on page 120.
- Licenses: Device license information is now available on the *Device Manager* > *License* pane. See License on page 135.
- WAN link load balancing: You can now create profiles to load-balance WAN links on the *Device Manager* > *WAN LLB* pane. See WAN Link Load Balance on page 173

Policy & Object improvements

The *Policy & Objects* pane includes the following improvements:

- Each policy now requires a unique name.
- You can now find unused objects.
- You can now delete address, service, and schedule objects that are used by a policy.
- You can now find duplicate objects and optionally merge duplicate objects into one object.
- You can now edit objects inline for a policy by using the *Object Selector* frame.

See Policy & Objects on page 187.

AP management improvements

You can now manage FortiAP devices that are controlled by FortiGate devices by using the *AP Manager* pane. You can discover, authorize, and monitor access points. You can also create and assign SSIDs. You must add the FortiGate devices to FortiManager to use the *AP Manager* pane for FortiAP devices. See AP Manager on page 261.

FortiClient endpoint monitoring

FortiClient management is now available on the *FortiClient Manager* pane. You can create FortiClient profiles and install the profiles to endpoints via FortiGate devices. You can also monitor FortiClient endpoints that are registered to FortiGate devices. See FortiClient Manager on page 289.

VPN management

You can now manage IPsec VPNs and SSL-VPNs on the *VPN Manager* pane. On the *VPN Manager* pane, you can enable central VPN management, create VPN communities, and add devices to the communities. See VPN Manager on page 241.

In addition, FortiManager now includes a local CA server for each ADOM that simplifies VPN management. You can create certificate templates that use the local FortiManager CA server. When you assign a device to an SSL-VPN topology with a certificate template that uses the local FortiManager CA server, the certificate is automatically signed and installed to the FortiGate device. See Certificate templates on page 142.

FortiAnalyzer features

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

- *FortiView*
- *Log View*
- *Event Monitor*
- *Reports*

For information about using FortiAnalyzer features, see the *FortiAnalyzer Administration Guide*.

Expanded XML API

FortiManager includes a new XML API. More functions are available and the method of communication between FortiManager and the XML API is more efficient. You can download the WSDL files for the new XML API from the *System Settings* > *Advanced* > *Advanced Settings* page. See Advanced settings on page 371.

For more information, see the *FortiManager XML API Reference Guide*.

FortiManager Architecture

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

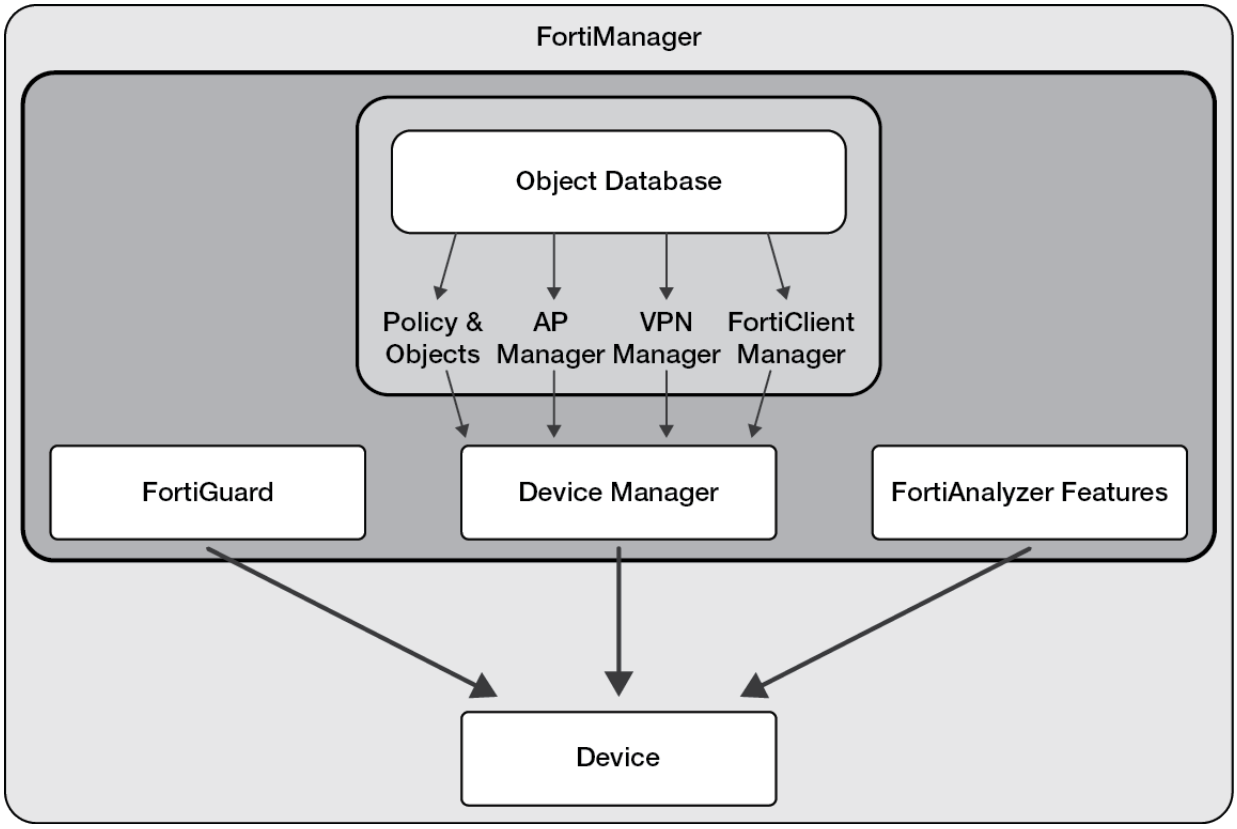
To reduce network delays and to minimize external Internet usage, a FortiManager installation can also act as an on-site FortiGuard Distribution Server (FDS) for your managed devices and FortiClient agents to download updates to their virus and attack signatures, and to use the built-in web filtering 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 up to 5000 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.

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

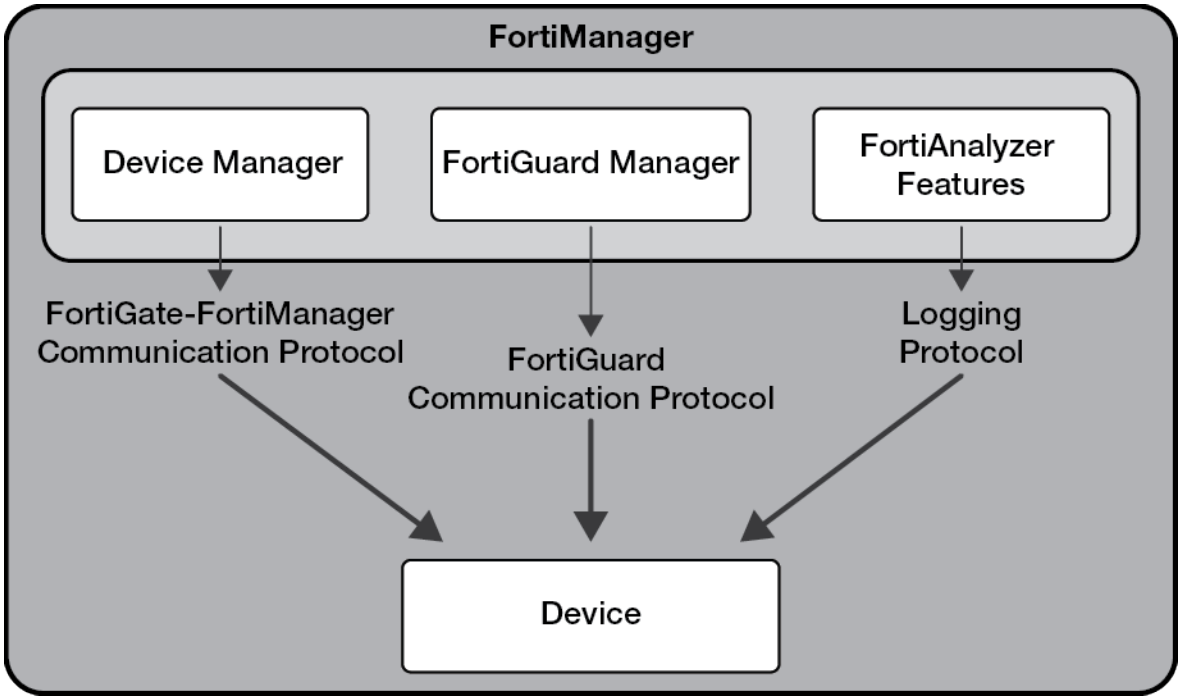


Inside the FortiManager system

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 Device Manager on page 94.

FortiGuard Manager

FortiGuard Manager communicates with devices by using the FortiGuard protocol.

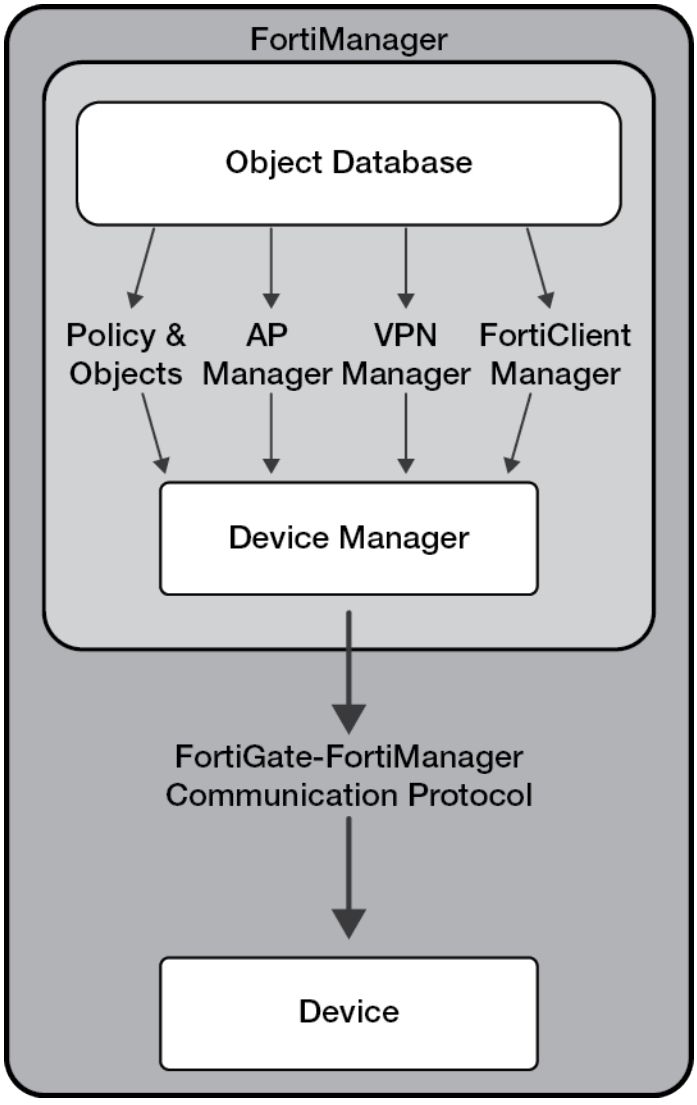
FortiAnalyzer features

When FortiAnalyzer features are enabled for the FortiManager unit, the *FortiView*, *Log View*, *Event Monitor*, 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*



Policy & Objects

The *Policy & Objects* pane contains all of your global and local policy packages and objects, and configuration revisions. Objects created for the *Policy & Objects* pane are stored in the objects database.See Policy & Objects on page 187.

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 AP Manager on page 261.

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 Manager on page 241.

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 VPN Manager on page 241.

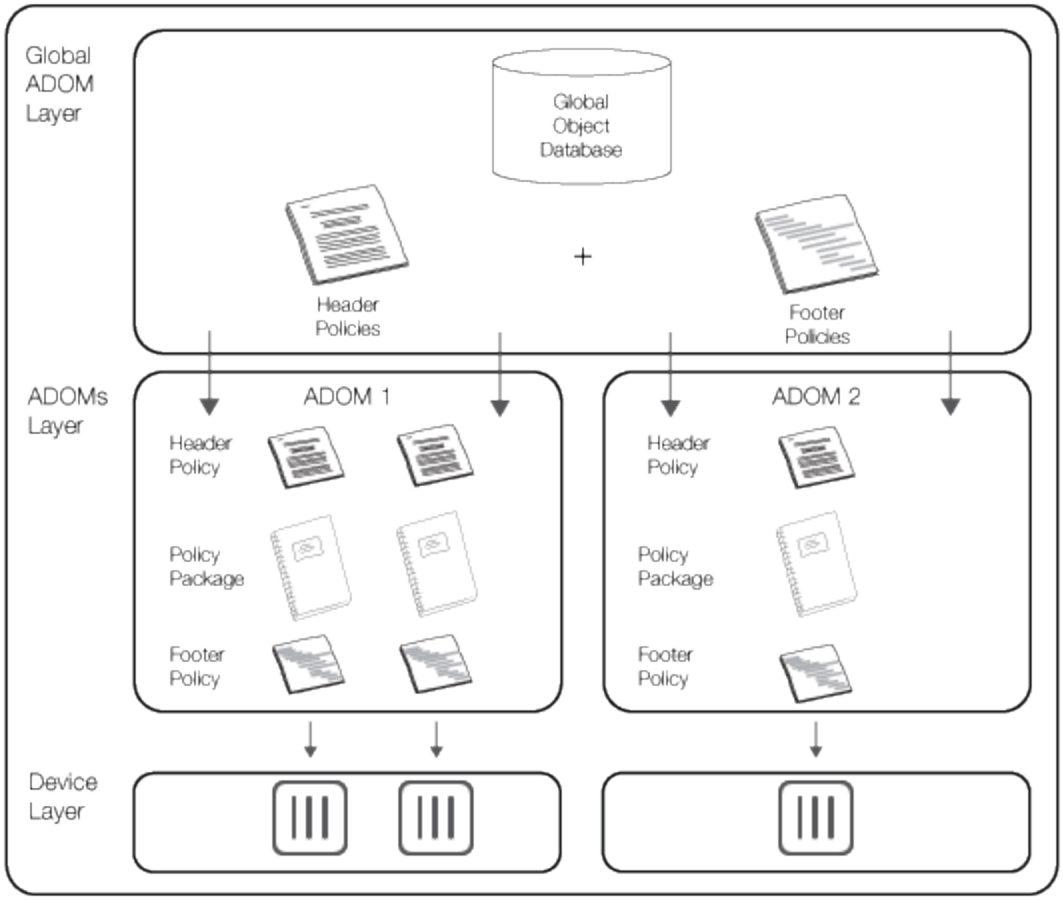
ADOMs and devices

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.

Key features of the FortiManager system

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 49.

Local FortiGuard service provisioning

A FortiGate device can use the FortiManager unit for antivirus, intrusion prevention, web filtering, and email filtering to optimize performance of rating lookups, and definition and signature downloads. See FortiGuard on page 303.

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 143.

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.

See also Overview on page 30.

Overview

This section provides an overview of configuring a FortiManager device. It also provides an overview of adding devices to FortiManager as well as configuring and monitoring managed devices.

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

Configuring the FortiManager

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

To configure FortiManager devices:

1. Connect to the GUI. See Connecting to the GUI on page 33.
2. Configure IP addresses. See Configuring network interfaces on page 40.
3. Configure the RAID level, if the FortiManager unit supports RAID. See Configuring RAID on page 46.

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 137 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 Configuring ADOMs on page 52.
3. Configure administrator accounts. See Configuring administrator accounts on page 66.
4. Add devices to FortiManager. See Adding devices on page 95.
5. If not done when you added the device, import the policy from each online device to FortiManager. See Import policy wizard on page 103.

   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.

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 231or Edit an object on page 233.
2. Create or edit policies in a policy package to select the objects. See Managing policies on page 201.
   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 193.
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 110.
5. Install the policy package and device settings to devices by using the Installation Wizard. See Installing to devices on page 115.

Enabling central management

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

- WAN link load balance—see WAN Link Load Balance on page 173
- VPN—see VPN Manager on page 241

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

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

To use central management:

1. Enable central management for WAN link load balance and/or VPN.
2. Configure the settings.
3. Install the settings to one or more devices.

Monitoring managed devices

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

- Quick status bar—see Using the quick status bar on page 120
- Device dashboard—see Using the device dashboard on page 110
- Device configurations—see Managing device configurations on page 125
- Policy packages—see Managing policy packages on page 192
- *AP Manager* pane—see Monitor on page 272
- *FortiClient Manager* pane—see Monitoring FortiClient endpoints on page 293

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

- *WAN LLB* pane—see WAN Link Load Balance on page 173
- *VPN Manager* pane—see Monitor IPsec VPN communities on page 250and Monitor SSL-VPN on page 258

When FortiAnalyzer features are enabled on the FortiManager device, you can also view and analyze log messages from managed devices by using the *FortiView*, *Log View*, *Event Monitor*, and *Reports* panes. See FortiAnalyzer Features on page 323.

GUI

This section describes general information about using the GUI to access the Fortinet system from within a current web browser.

This section includes the following topics:

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.

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*.
5. If ADOMs are enabled, the *Select an ADOM* pane is displayed. Click an ADOM to select it.
   The FortiManager home page is displayed.
6. Click a tile to go to that pane.

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 the network on page 40.

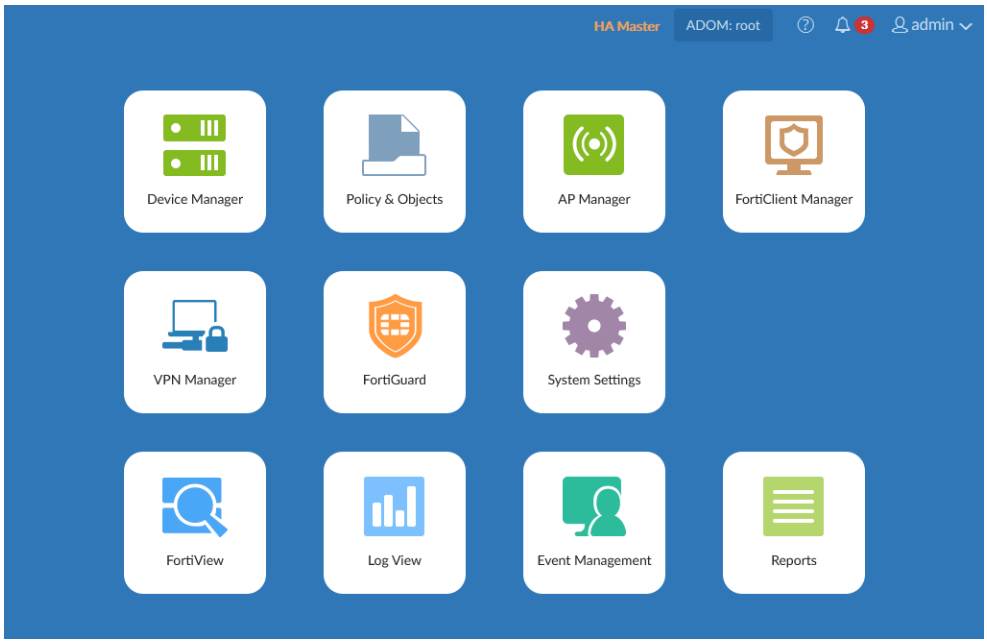
If the URL is correct and you still cannot access the GUI, you may also need to configure static routes. For details, see .

When the system is busy during a database upgrade or rebuild, you will receive a message in the GUI log in screen. 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 Configuring administrator accounts on page 66.

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 will vary depending on the privileges of the current user.

Device Manager	• Manage devices, VDOMs, groups, firmware images, device licenses, and scripts, • Configure system, threat weight, FortiClient, and Certificate templates, and • View real-time monitor data. For more information, see Device Manager on page 94.
Policy & Objects	Configure policy packages and objects. For more information, see Policy & Objects on page 187.
AP Manager	Configure and manage FortiAP access points. For more information, see AP Manager on page 261.

FortiClient Manager	Manage FortiClient profiles and monitor FortiClient endpoints that are registered to FortiGate devices.
VPN Manager	Configure and manage VPN connections. You can create VPN topologies and managed/external gateways. For more information, see VPN Manager on page 241.
FortiGuard	Manage communication between devices and the FortiManager using the FortiGuard protocol.
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 325.
FortiView	View FortiView summary views for logging devices. This tab can be hidden by disabling the FortiAnalyzer feature set.
Log View	View logs for logging devices. This tab can be hidden by disabling the FortiAnalyzer feature set.
Event Monitor	Configure and view events for logging devices. This tab can be hidden by disabling the FortiAnalyzer feature set.
Reports	Configure and generate reports for logging devices. This tab can be hidden by disabling the FortiAnalyzer feature set.

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 drop-down 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. See Administrative Domains on page 49.
Help	Click to open the FortiManager online help, or view the *About* information for your device (Product, Version, and Build Number).
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.

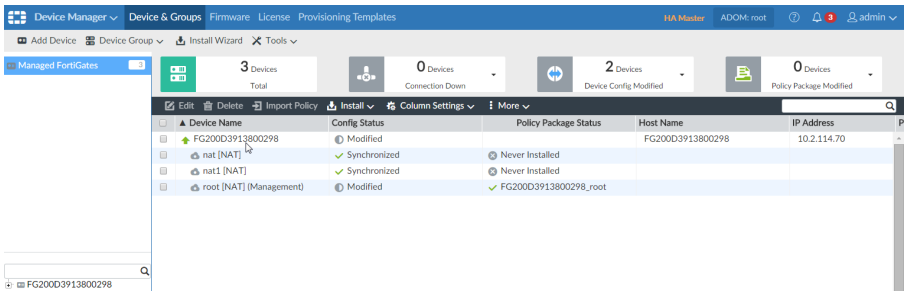
Panes

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

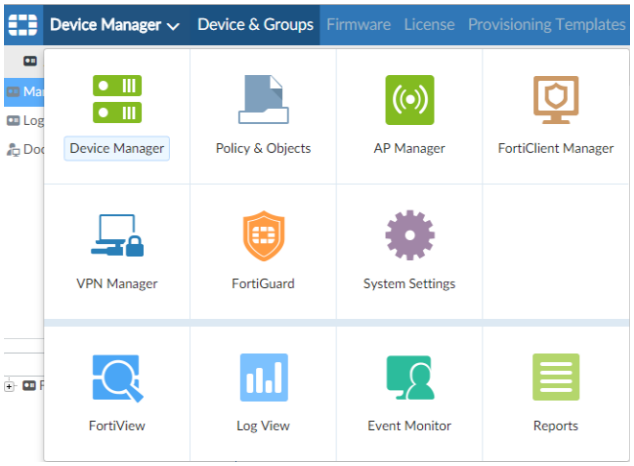
Banner	Along the top of the page; includes the home button (Fortinet logo), tile menu, ADOM menu (when enabled), admin menu, notifications, and help button.

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 *Create New* and *Delete*.

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 Device Manager on page 94 for more information.



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 Configuring global administrative settings on page 88.

Full-screen mode

You can view several panes in full-screen mode. When a pane is in full-screen mode, 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

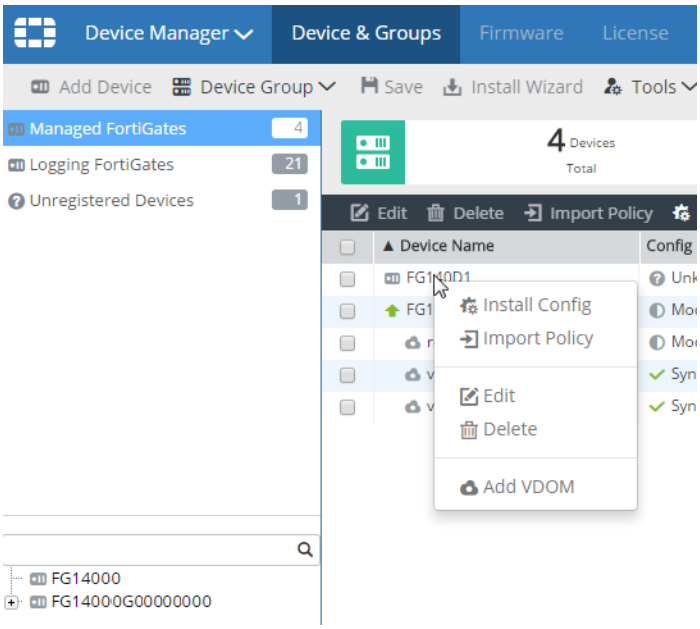
When ADOMs are enabled, you can move between ADOMs by selecting an ADOM from the *ADOM* menu in the banner.

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 Configuring administrator accounts on page 66 for more information.

Using the right-click menu

Options are sometimes also available by using a right-click menu. You can right-click items in the content pane to display a menu and access the options.

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*, and so on.



Security considerations

This section includes the following topics:

- Restricting GUI access by trusted host
- Other security considerations

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 Configuring administrator accounts on page 66 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.

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* widget, enter the following command:
```
execute reboot
The system will be rebooted.
Do you want to continue? (y/n)
```
2. Enter *y* to continue. The FortiManagersystem 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* widget, 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* widget, 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* widget, 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.

Network

Configuring the network

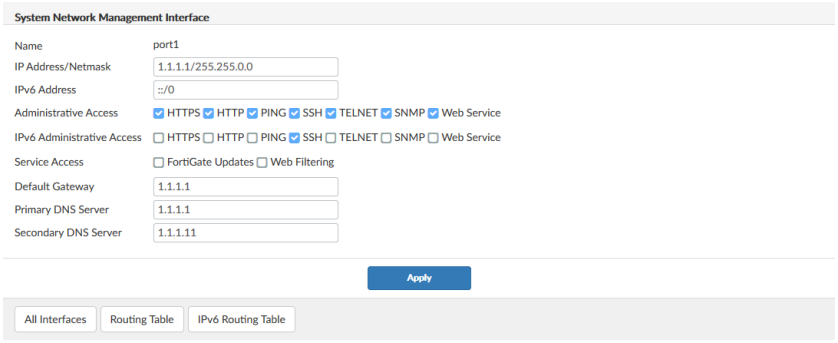
Configuring network interfaces

The FortiManager unit can manage Fortinet devices connected to any of its interfaces. If the FortiManager unit is operating as part of an HA cluster, it is recommended to dedicate interfaces for the HA connection / synchronization when possible. However, it is possible to use the same interfaces for both HA and device management.

The DNS servers must be on the networks to which the FortiManager unit connects, and should be two different addresses

To view the configured network interfaces,

1. Go to *System Settings* > *Network*. The *System Network Management Interface* pane is displayed.



2. Configure the settings for *port1*, and click *Apply*. For a description of the options, see System Network Management Interface pane on page 42.

Adding a static route

To add a static route:

1. Go to *System Settings* > *Network*.
2. Click the *Routing Table* button or the *IPv6 Routing Table* button, and click *Create New*. The *Create New Network Route* pane is displayed.
3. Configure the options, and click *OK*. For a description of the options, see Create New Network Route pane on page 42.

Managing the network

Viewing the network interface list

To view the network interface list:

1. Go to *System Settings* > *Network*.
2. Click the *All Interfaces* button.

Editing network settings

To edit network settings:

1. Go to *System Settings* > *Network*.
2. Click *All Interfaces*, *Routing Table*, or *IPv6 Routing Table*.
3. Select and entry, and click *Edit*. The *Edit System Interface* pane is displayed.
4. Configure the settings, and click *OK*. For a description of the options, see Edit System Interface pane on page 42.

Changing administrative access

Administrative access enables an administrator to connect to the FortiManager system to view and change configuration settings. The default configuration of your FortiManager system allows administrative access to one or more of the interfaces of the unit as described in your FortiManager system *QuickStart Guide* and *Install Guide* available in the Fortinet Document Library.

Administrative access can be configured in IPv4 or IPv6 and includes the following settings:

HTTPS	PING	TELNET	Web Service
HTTP	SSH	SNMP	

To change administrative access to your FortiManager system:

1. Go to *System Settings* > *Network*.
   Administrative access is configured for port1. To configure administrative access for another interface, click *All Interfaces*, and then select the interface to edit.
2. Set the *IPv4 IP/Netmask* or *IPv6 Address*.
3. Select one or more *Administrative Access* types for the interface.
4. Select *Service Access*, *FortiGate Updates*, and *Web Filtering/Antispam* if required.
5. Set the *Default Gateway*.
6. Configure the primary and secondary DNS servers.
7. Click *Apply*.
   In addition to the settings listed earlier, you can select to enable access on interface from the *All Interfaces* window.

Network references

System Network Management Interface pane

Following is a description of the fields on the *System Settings* > *Network* pane when creating an interface.

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, Telnet, SNMP, and Web Service.
IPv6 Administrative Access	Select the allowed IPv6 administrative service protocols from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, and Web Service.
Service Access	Select the Fortinet services that are allowed access on this interface. These include *FortiGate Updates* and *Web Filtering*. By default all service access is enabled on port1, and disabled on port2.
Default Gateway	The default gateway associated with this interface.
Primary DNS Server	Type the primary DNS server IP address.
Secondary DNS Server	Type the secondary DNS server IP address.

Create New Network Route pane

Following is a description of the fields on the *System Settings* > *Network* pane when creating a static route.

Destination IP/Mask	Type the destination IP address and netmask for this route.
Gateway	Type the IP address of the next hop router to which this route directs traffic.
Interface	Select the network interface that connects to the gateway.

Edit System Interface pane

Following is a description of the fields on the *System Settings* > *Network* page when editing an interface.

Name	Displays the name of the interface.
Alias	Type an alias for the port to make it easily recognizable.

IP Address/Netmask	Type the IP address and netmask for the interface.
IPv6 Address	Type the IPv6 address for the interface.
Administrative Access	Select the services to allow on this interface. Any interface that is used to provide administration access to the FortiManager unit will require at least HTTPS or HTTP for GUI access, or SSH for CLI access.
IPv6 Administrative Access	Select the services to allow on this interface. Any interface that is used to provide administration access to the FortiManager unit will require at least HTTPS or HTTP for GUI access, or SSH for CLI access.
Service Access	Select the Fortinet services that are allowed access on this interface. These include *FortiGate Updates* and *Web Filtering*. By default all service access is enabled on port1, and disabled on port2.
Status	Enable or disable the interface. Click *Enable* to enable the interface and allow the interface to accept network traffic. Click *Disable* to disable the interface.

RAID management

RAID helps to divide data storage over multiple disks, providing increased data reliability. FortiManager units that contain multiple hard disks can have RAID configured for capacity, performance, and availability.

Supported RAID levels

FortiManager units with multiple hard drives can support the following 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.

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 several backup hard disks available.

RAID 1 +Spare

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.

RAID 5 +Spare

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.

RAID 6 +Spare

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.

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.

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. It requires at least eight disks.

Configuring RAID

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.

If the RAID setting is changed, all data will be deleted.

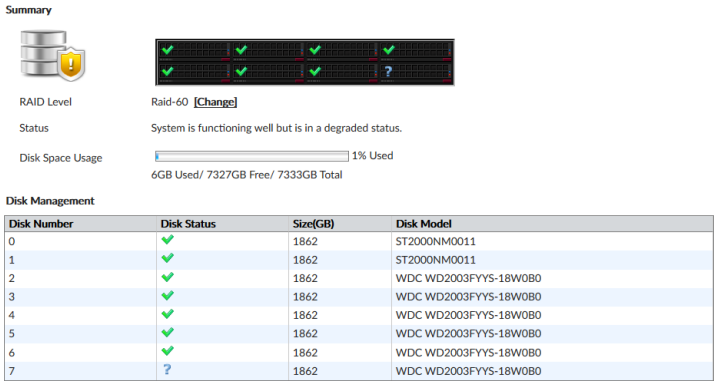
Managing RAID

You can monitor RAID status, swap hard disks, and in some cases, add new disks to the FortiManager unit.

Monitoring RAID status

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 336.

To view the RAID status, go to *System Settings* > *RAID Management*. The RAID Management pane displays the status of each disk in the RAID array, including the disk's RAID level. You can also see how much disk space is being used. For a description of the fields, see RAID references on page 48.



Hot 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, also known as hot swapping. On FortiManager units with software RAID, the device must be shutdown prior to exchanging the hard disk.

FortiManager 1000 series devices and below do not support hot swapping. For more information, see the *Replacing Hard Drives Guide*.

To identify which hard disk failed, read the relevant log message in the *Alert Message Console* widget (see Alert Messages Console widget on page 336).

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 has 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:

Remove the faulty hard disk, and replace it with a new one.

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 check mark icon for all disks and the *RAID Status* area displays the progress of the RAID re-synchronization/rebuild.

Once a RAID array is built, adding another disk with the same capacity will not affect the array size until you rebuild the array by restarting the FortiManager unit.

Adding new disks

Some FortiManager units have space to add more hard disks to increase your storage capacity.

Fortinet recommends that 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 exactly 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 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.

4. Configure the RAID level.
5. If you backed up the log data, restore the data.

RAID references

RAID Management page

Following is a description of the fields on the *System Settings* > *RAID Management* pane.

Summary		
	Graphic	Displays the position and status of each disk in the RAID array. Hover the mouse cursor over a disk to view the disk number, model, firmware version, level, capacity, and status.
	RAID Level	Displays the selected RAID level.
	Change	Click 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		Displays information about each disk in the RAID array.
	Disk Number	Identifies the disk number for each disk in the RAID array.
	Disk Status	Displays the status of each disk in the RAID array.
	Size (GB)	Displays the size in GB of each disk in the RAID array.
	Disk Model	Displays the model number of each disk in the RAID array.

Administrative Domains

FortiManager appliances scale to manage thousands of Fortinet devices. Administrative domains (ADOMs) enable administrators to manage only those devices that they are specifically assigned, based on the ADOMs to which they have access. FortiGate devices with multiple VDOMs can be divided among multiple ADOMs.

If ADOMs are enabled, 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. Administrator accounts that have special permissions, such as the `admin` account, can see and maintain all ADOMs and the devices within those domains.

ADOMs are not enabled by default, and enabling and configuring the domains can only be performed by the `admin` administrator.

The maximum number of ADOMs you can add depends on the FortiManager system model. Please refer to the FortiManager data sheet for information on the maximum number of devices that your model supports.

What is the best way to organize my devices using ADOMs?

You can organize devices into ADOMs to allow you to better manage these devices. You can organize these devices by:

- 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.

Non-FortiGate devices are automatically located in specific ADOMs for their device type. They cannot be moved to other ADOMs.

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 consider *Read Only*, where you are not able to make changes to the ADOM and managed devices from the 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.

Backup mode enables you to configure an ADOM where all the devices that are added to the ADOM will only have their configuration backed up. Configuration changes cannot be made to the devices in 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.

ADOM versions

ADOMs can concurrently manage FortiGate units running FortiOS 5.0, 5.2 and 5.4, allowing devices running these versions to share a common database. This allows you to continue to manage an ADOM as normal while upgrading the devices within that ADOM.

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.

FortiManager 5.4 supports FortiOS 5.0, 5.2, and 5.4 ADOMs. For a complete list of supported devices and firmware versions, see the FortiManager Release Notes.

Each ADOM is associated with a specific FortiOS version, based on the firmware version of the devices that are in that ADOM. This version is selected when creating a new ADOM (see Creating ADOMs on page 52), and can be updated only after all of the devices within the ADOM have been updated to the same FortiOS firmware version.

The general steps for upgrading an ADOM that contains multiple devices running FortiOS 5.2 from 5.2 to 5.4 are as follows:

1. In the ADOM, upgrade one of the FortiGate units to FortiOS 5.4, and then resynchronize the device. See Firmware on page 133 for more information.
   All of the ADOM objects, including Policy Packages, remain as 5.2 objects.
2. Upgrade the rest of the FortiGate units in the ADOM to FortiOS 5.4.
3. Upgrade the ADOM to 5.4. See Upgrading an ADOM on page 57 for more information.
   All of the database objects will be converted to 5.4 format, and the GUI content for the ADOM will change to reflect 5.4 features and behavior.

An ADOM can only be upgraded after all the devices within the ADOM have been upgraded.

In FortiManager 5.4.3 and later, the root ADOM can be updated without enabling ADOMs.

In FortiManager 5.2.1 and later, FortiOS 5.0 and 5.2 share a common policy package database. You can upgrade a 5.0 ADOM to 5.2.
In FortiManager 5.4.1 and later, FortiOS 5.2 and 5.4 share a common policy package database. You can upgrade a 5.2 ADOM to 5.4.

Global database version

The global database is reset when the database version is edited. The database is not reset when the global database ADOM is upgraded using the *Upgrade* command.

The global database ADOM should only be upgraded after all the ADOMs that are using a global policy package have been upgraded.

To upgrade the global database ADOM:

1. Go to *System Settings* > *All ADOMs*.
2. Select *Global Database* then click *More* > *Upgrade* in the toolbar, or right-click *Global Database* and select *Upgrade*.
   If the ADOM has already been upgraded to the latest version, this option will not be available.
3. Click *OK* in the *Upgrade ADOM* dialog box.
4. After the upgrade finishes, click *Close* to close the dialog box.

To edit the global database version:

Editing the global database version will reset the database. All global policy packages will be lost. This should only be used when starting to use the global database for the first time, or when resetting the database is required.

1. Go to *System Settings* > *All ADOMs*.
2. Select *Global Database* then click *Edit* in the toolbar, or right-click *Global Database* and select *Edit*. The *Edit Global Database* window opens.
3. Select the version.
4. Click *OK* to save the setting.
5. A confirmation dialog box will be displayed. Click *OK* to continue.

Configuring ADOMs

To create and configure ADOMs, go to *System Settings* > *All ADOMs*.

Enabling and disabling the ADOM feature

To enable or disable the ADOM feature, you must be logged in as the `admin` administrator. Only this user has the ability to enable or disable this feature.

The ADOMs feature cannot be disabled if ADOMs are still configured and listed, and they still have managed devices within them.

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 as `admin`.
2. Go to *System Settings* > *Dashboard*.
3. In the *System Information* widget, toggle the *Administrative Domain* switch to *ON*. You will need to log back in to the FortiManager.

To disable the ADOM feature:

1. Remove all the managed devices from all ADOMs.
2. Delete all non-root ADOMs by going to *System Settings* > *All ADOMs*, select each ADOM, then click *Delete*. 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*.

Creating ADOMs

To add an ADOM, you must be logged in as the `admin` administrator. You must also first enable administrative domains in the GUI; see Enabling and disabling the ADOM feature on page 52.

To create an ADOM

1. Go to *System Settings* > *All ADOMs*.
2. Click *Create New*. The *Create New ADOM* pane is displayed.

3. Configure the following settings:

Name	Type a name that will allow you to distinguish this ADOM from your other ADOMs. ADOM names must be unique.
Type	Select either FortiGate or FortiCarrier from the drop-down menu. Other devices types are added to their respective default ADOM upon registering with FortiManager.
Version	Select the version of FortiGate devices in the ADOM. FortiManager supports FortiOS 5.6, 5.4, and 5.2. For information on supported device firmware version, see the *FortiManager Release Notes*.
Devices	Add a device or devices with the selected version to this ADOM.
Search	Search for a device.
Central Management	Select the *VPN* check box to enable central VPN management. Clear the check box to disable the feature. Select the *WAN Link Load Balance* check box to enable central WAN link load balancing. Clear the check box to disable the feature.
Mode	Select *Normal* mode if you want to manage and configure the connected FortiGate devices from the FortiManager GUI. Select *Backup* mode if you want to backup the FortiGate configurations to the FortiManager, but configure each FortiGate locally.
Default Device Selection for Install	Select either *Select All Devices/Groups* or *Specify Devices/Groups*. This option is only available when the *Mode* is *Normal*.
Data Policy	Use the *Data Policy* settings to specify how long to keep logs in the indexed and compressed states. This section is only available when FortiAnalyzer features are enabled. See Enable or disable FortiAnalyzer features on page 334. For more information, see the *FortiAnalyzer Administration Guide*, available in the Fortinet Document Library.
Disk Utilization	Use the *Disk Utilization* settings to specify how much disk space to use for logs. This section is only available when FortiAnalyzer features are enabled. See Enable or disable FortiAnalyzer features on page 334. For more information, see the *FortiAnalyzer Administration Guide*, available in the Fortinet Document Library.

4. Click *OK* to create the ADOM.

   The number of ADOMs that can be created is dependent on the FortiManager model and its supported value. For more information on ADOM support values, see the FortiManager data sheet at http://www.fortinet.com/products/fortimanager/index.html.

Assigning devices to an ADOM

The admin administrator selects the devices to be included in an ADOM. You cannot assign the same device to two different ADOMs.

To assign devices to an ADOM:

1. Go to *System Settings* > *All ADOMs*.
2. Select the ADOM, and click *Edit*. The *Edit ADOM* pane is displayed.
3. Click *Select Device*. The *Select Device* pane is displayed.
4. Select the devices that you want to add. Only devices with the same version as the ADOM can be added. The selected devices are displayed in the *Devices* list.
5. When done selecting devices, click *Close* to close the *Select Device* pane.
6. Click *OK*.

You can add devices, device groups, and provision devices using the FortiManager wizards. For more information, see Adding devices with the wizard on page 96.

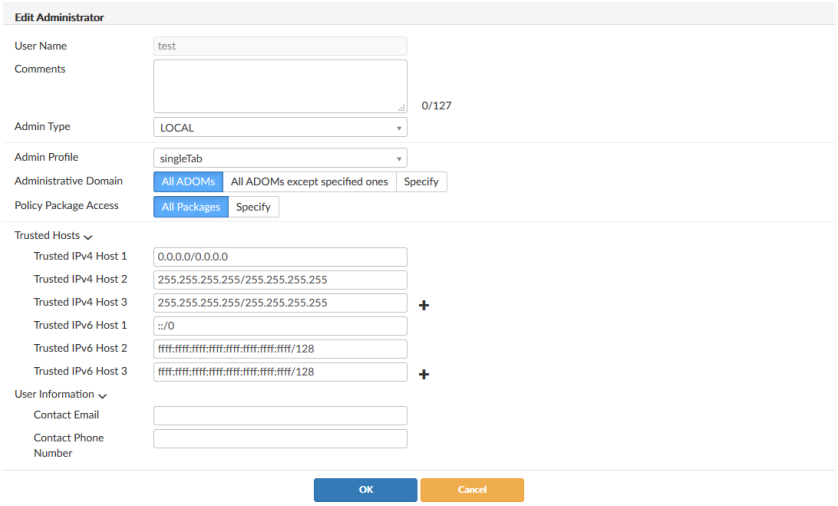
Assigning administrators to an ADOM

The adminadministrator 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 that 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 Configuring ADOMs on page 52.

To assign an administrator to specific ADOMs:

1. Log in as admin. Other administrators cannot configure administrator accounts when ADOMs are enabled.
2. Go to *System Settings* > *Admin* > *Administrator*.
3. Select an administrator, and click *Edit*. You can specify the *Administrative Domain* and *Policy Package Access*.



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.

Managing ADOMs

To manage ADOMs, go to *System Settings* > *All ADOMs*.

ADOM device modes

An ADOM has two device modes: normal and advanced.

In normal mode, you cannot assign different FortiGate VDOMs to multiple FortiManager ADOMs. The FortiGate unit can only be added to a single ADOM.

In advanced mode, you can assign different VDOMs from the same FortiGate unit to multiple ADOMs. *Normal* mode is the default. To change from advanced back to normal, you must ensure no FortiGate VDOMs are assigned to an ADOM.

To change to a different device mode using the CLI, enter the following commands:

```
config system global
   set adom-mode {normal | advanced}
end
```

To change to a different device mode in the GUI, go to *System Settings* > *Advanced* > *Advanced Settings* and change *ADOM Mode* as required.

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 56

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, enter the following CLI commands in their entirety:

```
config system global
   set workspace-mode normal
end
```

To disable workspace mode, and enable concurrent ADOM access, enter the following CLI commands in their entirety:

```
config system global
   set workspace-mode disabled
      Warning: disabling workspaces may cause some logged in users to lose their unsaved
          data. Do you want to continue? (y/n) y
end
```

After changing the workflow mode, your session will end and you will be required to log back in to the FortiManager.

Locking an ADOM

If workspace is enabled, you must lock an ADOM prior to performing device-level changes to it. If you are making changes at the ADOM level, you can leave the ADOM unlocked and lock policy packages or objects independently.

The lock 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-prempt {enable | disable}
end
```

Upgrading an ADOM

To upgrade an ADOM, you must be logged in as the `admin` administrator.

An ADOM can only be upgraded after all the devices within the ADOM have been upgraded. See ADOM versions on page 50 for more information.

To upgrade an ADOM:

1. Go to *System Settings* > *All ADOMs*.
2. Either right-click on an ADOM and select *Upgrade*, or select the ADOM 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.

Deleting an ADOM

To delete an ADOM, you must be logged in a super-user administrator (see Administrator profiles on page 78), such as the *admin* administrator.

Prior to deleting an ADOM:

- All devices must be removed from the ADOM. See Assigning devices to an ADOM on page 54.
- Global policy packages assigned to the ADOM must be unassigned. See Assign a global policy package on page 194.

- References to the ADOM must be removed from administrator accounts (or the accounts deleted). See Assigning administrators to an ADOM on page 54.

To delete an ADOM

1. From the ADOM list at *System Settings* > *All ADOMs*
2. Select the ADOM(s), and click *Delete*.
3. In the confirmation dialog box, click *OK*.

Workflow Mode

Workflow mode is used to control the creation, configuration, and installation of policies and objects. It helps to ensure that 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, object, or device 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 or disable workflow mode

Workflow mode can only be enabled or disabled from the CLI.

After changing the workflow mode, your session will end, and you will be required to log back in to the FortiManager.

To enable or disable 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 | disable}
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.

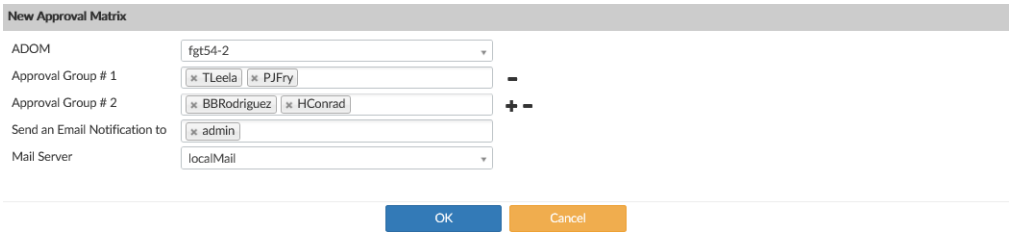
Up to eight approval groups can be added to an approval matrix. One user from each approval group must approve the changes before they are accepted. An approval email will automatically be sent to each member of each approval group when a change request is made.

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 363, and each administrator must have a contact email address configured, see Configuring administrator accounts on page 66.

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*.



3. Configure the following settings:

ADOM	Select the ADOM from the drop-down 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 drop-down list. A mail server must already be configured. See Mail server on page 363.

4. Click *OK* to create the approval matrix.

Workflow sessions

Administrators use workflow sessions to make changes to policies and objects. The session is then submitted for review and approval or rejection by the administrators defined in the ADOMs workflow approval matrix.

Administrators with the appropriate permissions will be able to approve or reject any pending requests. When viewing the session list, they can choose any pending sessions, and click the approve or reject buttons. They can also add a comment to the response. A notification will then be sent to the administrator that submitted the session and all of the approvers.

You cannot prevent administrators from approving their own workflow sessions.

If the session was approved, no further action is required. If the session was rejected, the administrator will need to either repair or discard the session.

The Global Database ADOM includes the *Assignment* option, for assigning the global policy package to an ADOM. Assignments can only be created and edited when a session is in progress. After a global database session is approved, the policy package can be assigned to the configured ADOM. A new session will be created on the assigned ADOM and automatically submitted; it must be approved for the changes to take effect.

A session can be discarded at any time before it is approved.

After multiple sessions have been submitted or approved, a previously approved session can be reverted to, undoing all the later sessions. This creates a new session at the top of the session list that is automatically submitted for approval.

A workflow approval matrix must be configure for the ADOM to which the session applies before a workflow session can be started. See Workflow approval on page 59.

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 lock 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 64.
5. Click *Create New Session*.

6. Enter a name for session, add a comment describing the session, then click *OK* to start the session. You can now make the required changes to the policy packages and objects. See Policy & Objects on page 187.

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.

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, and 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 59), 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 64.
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 64.
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 64.
4. Select a rejected session, then click *Repair*.
   A new session is created and started, with the changes from the rejected session, so that 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.

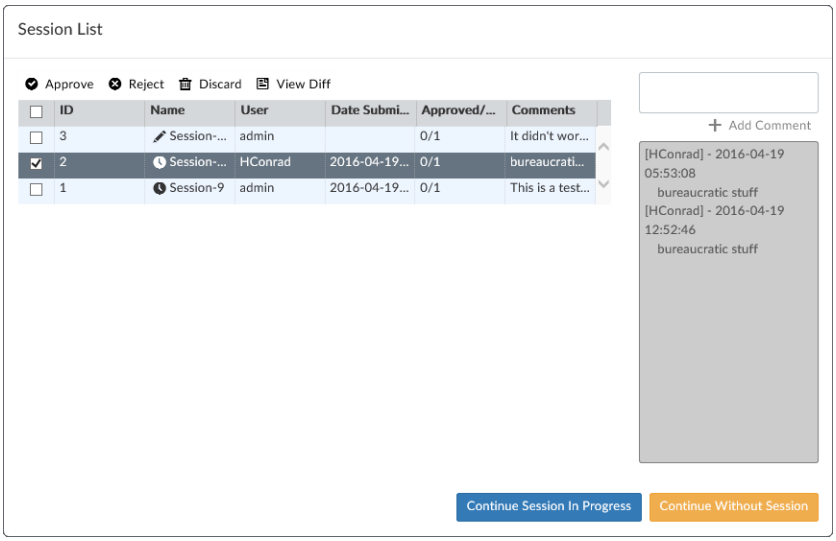
When a session is reverted, a new session is created and automatically submitted for approval.

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 64.
4. Select the session, then click *Revert*.

The session list

To view the session list, In *Policy & Objects*, go to *Sessions* > *Session List*. Different options will be available depending on the various states of the sessions (in progress, approved, etc.). When an ADOM is unlocked, only the comments and *View Diff* command are available.



The following options and information are available:

Approve	Approve the selected session. Enter comments in the *Approve Session* dialog box as required.
Reject	Reject the selected session. Enter comments in the *Reject Session* dialog box as required. A rejected session must be repaired before the next session in the list can be approved.
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 that 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 details to view specific changes within a policy package.
ID	A unique number to identify the session.
Name	The user-defined name to identify the session. The icon shows the status of the session: waiting for approval, approved, rejected, repaired, or in progress. Hover the cursor over the icon to see a description.

User	The administrator who created the session.
Date Submitted	The date and time that 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.

Administrator Accounts

The *System Settings* > *Admin* menu enables you to configure administrator accounts, access profiles, and adjust global administrative settings for the FortiManager unit. The following menu options are available:

Administrators	Select to configure administrative users accounts. For more information, see Configuring administrator accounts on page 66.
Profile	Select to set up access profiles for the administrative users. For more information, see Administrator profiles on page 78.
Approval Matrix	Select to create a new approval matrix or edit/delete an existing approval matrix. For more information, see Workflow approval on page 59.
Remote Auth Server	Select to configure authentication server settings for administrative log in. For more information, see Remote authentication server on page 83.
Admin Settings	Select to configure connection options for the administrator including port number, language of the GUI and idle timeout. For more information, see Global administrator settings on page 87.

Configuring administrator accounts

Go to *System Settings* > *Admin* > *Administrator* to view the list of administrators and configure administrator accounts. Only the default `admin` administrator account can see the complete administrators list. If you do not have certain viewing permissions, you will not see the administrator list.

The following information is available:

User Name	The name this administrator uses to log in. Select the administrator name to edit the administrator settings.
Type	The profile type. One of the following: LOCAL, RADIUS, LDAP, TACACS+, or PKI. When the administrator profile is a restricted administrator, this information will appear in the type column.
Profile	Select a profile from the list. The profile selected determines the administrator's access to the FortiManager unit's features. *Restricted_User* and *Standard_User* admin profiles do not have access to the *System Settings* tab. An administrator with either of these admin profiles will see a change password icon in the navigation pane.

ADOMs	Choose the ADOMs this administrator will be able to access, select *All ADOMs*, *All ADOMs except specified ones* or *Specify*. Select the remove icon to remove an Administrative Domain. This field is available only if ADOMs are enabled.The *Super_User* profile defaults to *All ADOMs* access.
Policy Packages	Choose either *All Packages* or *Specify*.
Status	Indicates whether the administrator is currently logged into the FortiManager unit not. An enabled icon indicates the administrator is logged in, a disabled icon indicates the administrator is not logged in.
Comments	Optionally, enter a description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account.
Email	The contact email address associated with the administrator.
Phone	The contact phone number associated with the administrator.
Trusted IPv4 Host	The IPv4 trusted host(s) associated with the administrator.
Trusted IPv6 Hosts	The IPv6 trusted host(s) associated with the administrator.

The following options are available:

Create New	Select to create a new administrator.
Edit	Select an administrator and select *Edit* from the toolbar to edit the entry. Alternatively, you can double-click the entry to open the *Edit Administrator* page.
Delete	Select the check box next to the administrator you want to remove from the list and select *Delete*.

To create a new local administrator account:

1. Go to *System Settings* > *Admin* > *Administrator*.
2. Click *Create New*.
3. Configure the following settings:

User Name	Type the name that this administrator uses to log in. This field is only editable when you are creating a new administrator account.
Comments	Optionally, type a description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account. Character limit: 127

Admin Type	Select LOCAL from the drop-down list.
New Password	Type the password.
Confirm Password	Type the password again to confirm it. The passwords must match.
Admin Profile	Select a profile from the drop-down menu. The profile selected determines the administrator's permission to the FortiManager unit's features. *Restricted_User* and *Standard_User* administrator profiles do not have access to the *System Settings* tab. An administrator with either of these administrator profiles will see a change password icon in the navigation pane. To create a new profile, see Creating custom administrator profiles on page 82.
Administrative Domain	Choose the ADOMs this administrator will be able to access. Select *All ADOMs*, *All ADOMs except specified ones*, or *Specify*. If you select *All ADOMs except specified ones* or *Specify*, click the add icon to identify Administrative Domains. Select the remove icon to remove an administrative domain from this list. When the *Admin Profile* is a restricted administrator profile, you can only select one administrative domain. This field is available only if ADOMs are enabled.
Policy Package Access	Choose the policy packages this administrator will have access to, or select *All Package*. Select *Specify* and then select the *Add* icon to add policy packages. Select the remove icon to remove a policy package from this list.This field is not available when the *Admin Profile* is a restricted administrator profile.
Trusted Hosts	Optionally, type the trusted host IPv4 or IPv6 address and netmask from which the administrator can log in to the FortiManager unit. Select the *Add* icon to add trusted hosts. You can specify up to ten trusted hosts. Select the delete icon to remove a policy package from this list. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see Using trusted hosts on page 77. Best practice: Restrict administrator access by trusted hosts to help prevent unwanted access.
User Information (optional)	
Contact Email	Type a contact email address for the new administrator. This email address is also used for workflow session approval email notifications.
Contact Phone Number	Type a contact phone number for the new administrator.

4. Click *OK* to create the new local administrator account.

For information on configuring restricted administrator profiles and accounts, see Restricted Administrator Profiles on page 82.

Configuring RADIUS administrator accounts

Remote Authentication and Dial-in User Service (RADIUS) servers provide authentication, authorization, and accounting functions. FortiManager units use the authentication and authorization functions of the RADIUS server. To use the RADIUS server for authentication, you must configure the server before configuring the FortiManager users or user groups that will need it.

If you have configured RADIUS support and a user is required to authenticate using a RADIUS server, the FortiManager unit sends the user's credentials to the RADIUS server for authentication. If the RADIUS server can authenticate the user, the user is successfully authenticated with the FortiManager unit. If the RADIUS server cannot authenticate the user, the FortiManager unit refuses the connection.

If you want to use a RADIUS server to authenticate administrators, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure the FortiManager unit to access the RADIUS server
- create the RADIUS user group
- configure an administrator to authenticate with a RADIUS server.

For information on configuring a RADIUS server for remote administrator authentication, see Remote authentication server on page 83.

To create a new RADIUS administrator account:

1. Go to *System Settings* > *Admin* > *Administrator*.
2. Click *Create New*. The *New Administrator* dialog box opens.
3. Configure the following settings:

User Name	Type the name that this administrator uses to log in.
Comments	Optionally, type a description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account. Character limit: 127
Admin Type	Select RADIUS from the drop-down list.
RADIUS Server	Select the RADIUS server from the drop-down list.
Wildcard	Select to enable wildcard.
New Password	Type the password. This field is hidden when *Wildcard* is enabled.
Confirm Password	Type the password again to confirm it. The passwords must match. This field is hidden when *Wildcard* is enabled.

Admin Profile	Select a profile from the drop-down menu. The profile selected determines the administrator's permission to the FortiManager unit's features. To create a new profile, see Creating custom administrator profiles on page 82.
Administrative Domain	Choose the ADOMs this administrator will be able to access. Select *All ADOMs*, *All ADOMs except specified ones*, or *Specify*. If you select *All ADOMs except specified ones* or *Specify*, click the add icon to identify Administrative Domains. Select the remove icon to remove an administrative domain from this list. When the *Admin Profile* is a restricted administrator profile, you can only select one administrative domain. This field is available only if ADOMs are enabled. Best practice: Restrict administrator access only to the specific ADOMs that they are responsible for.
Policy Package Access	Choose the policy packages this administrator will have access to, or select *All Package*. Select *Specify* and then select the *Add* icon to add policy packages. Select the remove icon to remove a policy package from this list.This field is not available when the *Admin Profile* is a restricted administrator profile.Best practice: Restrict administrator access only to the specific policy packages that they are responsible for.
Trusted Hosts	Optionally, type the trusted host IPv4 or IPv6 address and netmask from which the administrator can log in to the FortiManager unit. Select the *Add* icon to add trusted hosts. You can specify up to ten trusted hosts. Select the delete icon to remove a policy package from this list. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see Using trusted hosts on page 77. Best practice: Restrict administrator access by trusted hosts to help prevent unwanted access.
User Information (optional)	
Contact Email	Type a contact email address for the new administrator. This email address is also used for workflow session approval email notifications.
Contact Phone Number	Type a contact phone number for the new administrator.

4. Click *OK* to create the new RADIUS administrator account.

Configuring LDAP administrator accounts

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, printers, etc.

If you have configured LDAP support and an administrator is required to authenticate using an LDAP server, the FortiManager unit contacts the LDAP server for authentication. If the LDAP server cannot authenticate the administrator, the FortiManager unit refuses the connection.

If you want to use an LDAP server to authenticate administrators in your VDOM, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure an LDAP server
- create an LDAP user group
- configure an administrator to authenticate with an LDAP server.

For information on configuring an LDAP server for remote administrator authentication, see Remote authentication server on page 83.

To create a new LDAP administrator account:

1. Go to *System Settings* > *Admin* > *Administrator*.
2. Click *Create New*. The *New Administrator* dialog box opens.
3. Configure the following settings:

User Name	Type the name that this administrator uses to log in.
Comments	Optionally, type a description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account. Character limit: 127
Admin Type	Select LDAP from the drop-down menu.
LDAP Server	Select the LDAP server from the drop-down list.
Wildcard	Select to enable wildcard.
New Password	Type the password. This field is hidden when *Wildcard* is enabled.
Confirm Password	Type the password again to confirm it. The passwords must match.This field is hidden when *Wildcard* is enabled.
Admin Profile	Select a profile from the drop-down menu. The profile selected determines the administrator's permission to the FortiManager unit's features. To create a new profile, see Creating custom administrator profiles on page 82.

Administrative Domain	Choose the ADOMs this administrator will be able to access. Select *All ADOMs*, *All ADOMs except specified ones*, or *Specify*. If you select *All ADOMs except specified ones* or *Specify*, click the add icon to identify Administrative Domains. Select the remove icon to remove an administrative domain from this list. When the *Admin Profile* is a restricted administrator profile, you can only select one administrative domain. This field is available only if ADOMs are enabled. Best practice: Restrict administrator access only to the specific ADOMs that they are responsible for.
Policy Package Access	Choose the policy packages this administrator will have access to, or select *All Package*. Select *Specify* and then select the *Add* icon to add policy packages. Select the remove icon to remove a policy package from this list.This field is not available when the *Admin Profile* is a restricted administrator profile.Best practice: Restrict administrator access only to the specific policy packages that they are responsible for.
Trusted Hosts only	Optionally, type the trusted host IPv4 or IPv6 address and netmask from which the administrator can log in to the FortiManager unit. Select the *Add* icon to add trusted hosts. You can specify up to ten trusted hosts. Select the delete icon to remove a policy package from this list. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see Using trusted hosts on page 77. Best practice: Restrict administrator access by trusted hosts to help prevent unwanted access.
User Information (optional)	
Contact Email	Type a contact email address for the new administrator. This email address is also used for workflow session approval email notifications.
Contact Phone Number	Type a contact phone number for the new administrator.

4. Click *OK* to create the new LDAP administrator account.

Configuring TACACS+ authentication for administrators

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.

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 cannot authenticate the administrator, the connection is refused by the FortiManager unit.

If you want to use an TACACS+ server to authenticate administrators, you must configure the authentication before you create the administrator accounts. To do this you need to:

- configure the FortiManager unit to access the TACACS+ server
- create a TACACS+ user group
- configure an administrator to authenticate with a TACACS+ server.

For information on configuring a TACACS+ server for remote administrator authentication, see Remote authentication server on page 83.

To create a new TACACS+ administrator account:

1. Go to *System Settings* > *Admin* > *Administrator*.
2. Click *Create New*. The *New Administrator* dialog box opens.
3. Configure the following settings:

User Name	Type the name that this administrator uses to log in.
Comments	Optionally, type a description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account. Character limit: 127
Admin Type	Select TACACS+ from the drop-down menu.
TACACS+ Server	Select the TACACS+ server from the drop-down menu.
Wildcard	Select to enable wildcard.
New Password	Type the password. This field is hidden when *Wildcard* is enabled.
Confirm Password	Type the password again to confirm it. The passwords must match.This field is hidden when *Wildcard* is enabled.
Admin Profile	Select a profile from the drop-down menu. The profile selected determines the administrator's permission to the FortiManager unit's features. To create a new profile, see Creating custom administrator profiles on page 82.
Administrative Domain	Choose the ADOMs this administrator will be able to access. Select *All ADOMs*, *All ADOMs except specified ones*, or *Specify*. If you select *All ADOMs except specified ones* or *Specify*, click the add icon to identify Administrative Domains. Select the remove icon to remove an administrative domain from this list. When the *Admin Profile* is a restricted administrator profile, you can only select one administrative domain. This field is available only if ADOMs are enabled. Best practice: Restrict administrator access only to the specific ADOMs that they are responsible for.

Policy Package Access	Choose the policy packages this administrator will have access to, or select *All Package*. Select *Specify* and then select the *Add* icon to add policy packages. Select the remove icon to remove a policy package from this list.This field is not available when the *Admin Profile* is a restricted administrator profile.Best practice: Restrict administrator access only to the specific policy packages that they are responsible for.
Trusted Hosts	Optionally, type the trusted host IPv4 or IPv6 address and netmask from which the administrator can log in to the FortiManager unit. Select the *Add* icon to add trusted hosts. You can specify up to ten trusted hosts. Select the delete icon to remove a policy package from this list. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see Using trusted hosts on page 77. Best practice: Restrict administrator access by trusted hosts to help prevent unwanted access.
User Information (optional)	
Contact Email	Type a contact email address for the new administrator. This email address is also used for workflow session approval email notifications.
Contact Phone Number	Type a contact phone number for the new administrator.

4. Select *OK* to create the new TACACS+ administrator account.

Configuring PKI certificate authentication for administrators

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. To do this you need to:

- configure a PKI user
- create a PKI user group
- configure an administrator to authenticate with a PKI certificate.

To use PKI certificate authentication, you will need the following certificates:

- an X.509 certificate for the FortiManager administrator (administrator certificate)
- an X.509 certificate from the Certificate Authority (CA) which has signed the administrator's certificate (CA Certificate)

For information on configuring a PKI server for remote administrator authentication, see Remote authentication server on page 83.

To get the CA certificate:

1. Log into your FortiAuthenticator.
2. Go to *Certificate Management* > *Certificate Authorities* > *Local CAs*.

3. Select the certificate and select *Export* in the toolbar to save the `ca_fortinet.com` CA certificate to your management computer. The saved CA certificate's filename is `ca_fortinet.com.crt`.

To get the administrator certificate:

1. Log into your FortiAuthenticator.
2. Go to *Certificate Management* > *End Entities* > *Users*.
3. Select the certificate and select *Export* in the toolbar to save the administrator certificate to your management computer. The saved CA certificate's filename is `admin_fortinet.com.p12`. This PCKS#12 file is password protected. You must enter a password on export.

To import the administrator certificate into your browser:

1. In Mozilla Firefox, go to *Edit* > *Preferences* > *Advanced* > *Encryptions* > *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 that you saved to your management computer. 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.
3. Configure the following settings:

User Name	Type the name that this administrator uses to log in. This field is available if you are creating a new administrator account.
Comments	Optionally, type a description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account. (Character limit = 127)
Admin Type	Select PKI from the drop-down list.
Subject	Type a comment in the subject field for the PKI administrator.
CA	Select the CA certificate from the drop-down list.
Require two-factor authentication	Select to enable two-factor authentication, then enter and confirm a password.
Admin Profile	Select a profile from the drop-down menu. The profile selected determines the administrator's permission to the FortiManager unit's features. To create a new profile, see Creating custom administrator profiles on page 82.

Administrative Domain	Choose the ADOMs this administrator will be able to access, or select *All ADOMs*. Select *Specify* and then select the add icon to add Administrative Domains. Select the remove icon to remove an administrative domain from this list. This field is available only if ADOMs are enabled. When the *Admin Profile* is a restricted administrator profile, you can only select one administrative domain. Best practice: Restrict administrator access only to the specific ADOMs that they are responsible for.
Policy Package Access	Choose the policy packages this administrator will have access to, or select *All Package*. Select *Specify* and then select the *Add* icon to add policy packages. Select the remove icon to remove a policy package from this list.This field is not available when the *Admin Profile* is a restricted administrator profile.Best practice: Restrict administrator access only to the specific policy packages that they are responsible for.
Trusted Hosts	Optionally, type the trusted host IPv4 or IPv6 address and netmask from which the administrator can log in to the FortiManager unit. Select the *Add* icon to add trusted hosts. You can specify up to ten trusted hosts. Select the delete icon to remove a policy package from this list. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see Using trusted hosts on page 77. Best practice: Restrict administrator access by trusted hosts to help prevent unwanted access.
User Information (optional)	
Contact Email	Type a contact email address for the new administrator. This email address is also used for workflow session approval email notifications.
Contact Phone Number	Type a contact phone number for the new administrator.

4. Click *OK* to create the new administrator account.

PKI authentication must be enabled via the FortiManager CLI. Use the following commands:

```
config system global
   set clt-cert-reg enable
end
```

When connecting to the FortiManager GUI, you must use HTTPS when using PKI certificate authentication.

When both `set clt-cert-req` and `set admin-https-pki-required` are enabled, only PKI administrators can connect to the FortiManager GUI.

Using 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 both to 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. By default, Trusted Host 3 is set to this address.

Managing administrator accounts

You can manage administrator accounts from *System Settings* > *Admin* > *Administrator*.

Option	Description
Create New	Create a new administrator account.
Edit	Edit the selected administrator account.
Delete	Delete the selected administrator account. You cannot delete the default *admin* administrator account from the GUI.

Monitoring administrator sessions

The *Admin Session List* lets you view the list of administrators logged into the FortiManager unit. From this window you can also disconnect users if necessary.

To view logged in administrators on the FortiManager unit, go to *System Settings* > *Dashboard*. In the *System Information* widget, under *Current Administrators*, click the *Current Session List* button. The list of current administrator sessions appears.

The following information is available:

User Name	The name of the administrator account. Your session is indicated by *(current)*.
IP Address	The IP address where the administrator is logging in from. This field also displays the logon type (GUI, jsconsole, SSH, or telnet).

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).

To disconnect an administrator:

1. In the *Current Sessions List*, select the check box for each administrator session that you want to disconnect, and click *Delete*.
2. Click *OK* to confirm deletion of the session.

   The disconnected administrator will see the FortiManager logon screen when disconnected. They will not have any additional warning. It is a good idea to inform the administrator before disconnecting if possible should they be in the middle of important configurations for the FortiManager or another device.

Administrator profiles

The *System Settings* > *Admin* > *Profile* menu enables you to create or edit administrator profiles which are used to limit administrator access permissions to devices or system features. There are four pre-defined system profiles:

Package_User	Package user profile have read/write policy package and objects permissions enabled, and have read-only access for system and other permissions.
Restricted_User	Restricted user profiles have no system permissions enabled, and have read-only access for all device permissions.
Standard_User	Standard user profiles have no system permissions enabled, but have read/write access for all device permissions.
Super_User	Super user profiles have all system and device permissions enabled.

Restricted_User and *Standard_User* administrator profiles do not have access to the *System Settings* tab. An administrator with either of these administrator profiles will see a change password icon in the navigation pane. Although the *System Settings* tab is read-only for an administrator with a *Package_User* administrator profile, they are able to change their password in the *Admin* > *Administrator* page.

The below table lists permissions for the four predefined administrator profiles. When *Read/Write* is selected, the user can view and make changes to the FortiManager system. When *Read-Only* is selected, the user can only view information. When *None* is selected, the user can neither view or make changes to the FortiManager system. The administrator profile restricts access to both the FortiManager GUI and command line interfaces

Setting	Predefined Administrator Profiles			
	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 `fgd-center-advanced`	Read-Write	None	None	Read-Only
Device Manager `device-manager`	Read-Write	Read-Write	Read-Only	Read-Write
Add/Delete 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
Terminal Access `term-access`	Read-Write	Read-Write	Read-Only	Read-Only
Manage Device Configuration `device-config`	Read-Write	Read-Write	Read-Only	Read-Write

Setting	Predefined Administrator Profiles			
	Super User	Standard User	Restricted User	Package User
Provisioning Templates `device-profile`	Read-Write	Read-Write	Read-Only	Read-Write
WAN Link Load Balance `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
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
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

Setting	Predefined Administrator Profiles			
	Super User	Standard User	Restricted User	Package User
VPN Manager `vpn-manager`	Read-Write	Read-Write	Read-Only	Read-Write
FortiView `realtime-monitor`	Read-Write	Read-Write	Read-Only	Read-Only
Event Management `event-management`	Read-Write	Read-Write	Read-Only	Read-Only
Reports `report-viewer`	Read-Write	Read-Write	Read-Only	Read-Only

You cannot delete these profiles, but you can modify them. You can also create new profiles if required.

This guide is intended for default users with full permissions. If you create a profile with limited permissions it will limit the ability of any administrator using that profile to follow procedures in this Guide.

To view the list of configured administrator profiles, go to *System Settings* > *Admin* > *Profile* .

The following information is displayed:

Name	The administrator profile name. Select the profile name to view or modify existing settings. For more information about profile settings, see Creating custom administrator profiles on page 82.
Type	The profile type. Either *System Admin* or *Restricted Admin*.
Description	Provides a brief description of the system and device access permissions allowed for the selected profile.

The following options are available:

Create New	Select to create a custom administrator profile.
Edit	Right-click and select *Edit* from the menu to edit the entry. Alternatively, double-click the entry to open the *Edit Profile* page.
Delete	Select the check box next to the profile you want to delete and select *Delete*. Predefined profiles cannot be deleted. You can only delete custom profiles when they are not applied to any administrators.

Creating custom administrator profiles

You can modify one of the pre-defined profiles or create a custom profile if needed. Only administrators with full system permissions can modify the administrator profiles. Depending on the nature of the administrator's work, access level, or seniority, you can allow them to view and configure as much, or as little, as required.

For information on configuring restricted administrator profiles and accounts, see Restricted Administrator Profiles on page 82.

To create a custom system administrator profile:

1. Go to *System Settings* > *Admin* > *Profile* and select *Create New* from the toolbar.
2. Configure the following settings:

Profile Name	Type a name for this profile.
Description	Type 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 *System Admin*.
Settings	Select *None*, *Read-Only*, or *Read-Write* access as required for all the settings. By default, access for all settings is *None*.

3. Select *OK* to save the new profile.

Managing administrator profiles

You can manage administrator profiles from *System Settings* > *Admin* > *Profile*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click an administrator profile to display the menu.

Option	Description
Create New	Create a new administrator profile.
Edit	Edit an administrator profile.
Delete	Delete the selected administrator profile. You can only delete custom profiles that are not applied to any administrators. You cannot delete the default administrator profiles: Restricted_User, Standard_User, and Super_User.

Restricted Administrator Profiles

The restricted profile is used by the restricted administrator account. You can use restricted administrator accounts to provide delegated management of Web Filter profiles, Application Sensors, and Intrusion Protection

System (IPS) Sensors for a specific ADOM. These restricted administrators can view, edit, and install changes to their ADOM.

To create a custom restricted administrator profile:

1. Go to *System Settings* > *Admin* > *Profile* and select *Create New* from the toolbar.
2. Configure the following settings:

Profile Name	Type a name for this profile.
Description	Type 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 *Restricted Admin*.
Permission	Select which permissions to enable from *Web Filter Profile*, *Application Filter*, and *IPS Sensor*.

3. Select *OK* to save the new restricted administrator profile.

Restricted administrator accounts

Once you have configured the new restricted administrator profile, you can create a new restricted administrator account and apply the profile to the administrator account.

To create a new restricted administrator account:

1. Go to *System Settings* > *Admin* > *Administrator* and select *Create New* from the toolbar.
2. Set *Admin Profile* to *Restricted_User*, then configure the rest of the settings (see Configuring administrator accounts on page 66).
3. Select *OK* to create the new restricted administrator account.

Remote authentication server

The FortiManager system supports remote authentication of administrators using Adding an LDAP server, Adding a RADIUS server, and Adding a TACACS+ server servers. To use this feature, 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. Existing servers can be modified and deleted as required; see Managing remote authentication servers on page 86.

The following information is displayed:

Name	The name of the server.
Type	The server type. One of LDAP, RADIUS, or TACACS+.
ADOM	The administrative domain(s) which are linked to the remote authentication server.

Details	Details about the server, such as the IP address.

The following options are available:

Delete	Select the checkbox next to the server entry and then select *Delete* to remove the selected server. Select *OK* in the confirmation dialog box to proceed with delete action.
Edit	Select the checkbox next to the profile, right-click, and select *Edit* in the right-click menu to edit the entry. Alternatively, you can double-click the entry to open the *Edit Server* page.
Create New	Create a new server. Select one of LDAP Server, RADIUS Server, or TACACS+ Server from the drop-down list.

Adding an LDAP server

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. An LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

If you have configured LDAP support and require a user to authenticate using an LDAP server, the FortiManager unit contacts the LDAP server for authentication. To authenticate with the FortiManager unit, the user enters a user name and password. The FortiManager unit sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the FortiManager unit successfully authenticates the user. If the LDAP server cannot authenticate the user, the FortiManager unit refuses the connection.

For information on configuring a LDAP server for remote administrator authentication, see Configuring LDAP administrator accounts on page 70.

To add an LDAP server:

1. From *System Settings* > *Admin* > *Remote Auth Server*, select *Create New* > *LDAP*from the toolbar. The *New LDAP Server* window opens.
2. Configure the following information:

Name	Type a name to identify the LDAP server.
Server Name/IP	Type the IP address or fully qualified domain name of the LDAP server.
Port	Type the port for LDAP traffic. The default port is 389.
Common Name Identifier	The common name identifier for the LDAP server. Most LDAP servers use cn. However, some servers use other common name identifiers such as UID.

Distinguished Name	The distinguished name used to look up entries on the LDAP servers use. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. Selecting the *query distinguished name* icon will query the LDAP for the name and open the *LDAP Distinguished Name Query* window to display the results.
Bind Type	Select the type of binding for LDAP authentication. Select Simple, Anonymous or Regular from the drop-down menu.
User DN	When the *Bind Type* is set to *Regular*, type the user DN.
Password	When the *Bind Type* is set to *Regular*, type the password.
Secure Connection	Select to use a secure LDAP server connection for authentication.
Protocol	When *Secure Connection* is enabled, select either LDAPS or STARTTLS.
Certificate	When *Secure Connection* is enabled, select the certificate from the drop-down list.
Administrative Domain	Choose the ADOMs this server will be linked to, or select *All ADOMs*. Select *Specify* and then select the add icon to add Administrative Domains. Select the remove icon to remove an administrative domain from this list. This field is available only if ADOMs are enabled.

3. Select *OK* to save the new LDAP server entry.

Adding a RADIUS server

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 logon. The password is not stored on the FortiManager unit.

For information on configuring a RADIUS server for remote administrator authentication, see Configuring RADIUS administrator accounts on page 69.

To add a RADIUS server:

1. From *System Settings* > *Admin* > *Remote Auth Server*, select *Create New* > *RADIUS* from the toolbar.
2. Configure the following settings:

Name	Type a name to identify the RADIUS server.
Server Name/IP	Type the IP address or fully qualified domain name of the RADIUS server.

Port	Type the port for RADIUS traffic. The default port is 1812. Some RADIUS servers use port 1645.
Server Secret	Type the RADIUS server secret.
Secondary Server Name/IP	Type the IP address or fully qualified domain name of the secondary RADIUS server.
Secondary Server Secret	Type the secondary RADIUS server secret.
Authentication Type	Type the authentication type the RADIUS server requires. The default setting of *ANY* has the FortiManager unit try all the authentication types. Select one of: *ANY*, *PAP*, *CHAP*, or *MSv2*.

3. Select *OK* to save the new RADIUS server configuration.

Adding a TACACS+ server

TACACS+ 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.

For information on configuring a TACACS+ server for remote administrator authentication, see Configuring TACACS+ authentication for administrators on page 72.

To add a TACACS+ server:

1. From *System Settings* > *Admin* > *Remote Auth Server*, select *Create New* > *TACACS* from the toolbar.
2. Configure the following information:

Name	Type a name to identify the TACACS+ server.
Server Name/IP	Type the IP address or fully qualified domain name of the TACACS+ server.
Port	Type the port for TACACS+ traffic. The default port is 49.
Server Key	Type 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. The default setting of *auto* has the FortiManager unit try all the authentication types. Select one of: *auto*, *ASCII*, *PAP*, *CHAP*, or *MSCHAP*.

3. Select *OK* to save the new TACACS+ server entry.

Managing remote authentication servers

Remote authentication servers can be modified and deleted as required.

To modify an existing server configuration:

1. Select the name of the server and select *Edit* from the menu.
2. Modify the settings as required and select *OK* to apply your changes.

To delete an existing server configuration:

1. Select the server configuration or configurations that you need to delete, then select *Delete* from the toolbar.
2. Select *OK* in the confirmation dialog box to delete the server entry or entries.

You cannot delete a server entry if there are administrator accounts using it.

Global administrator settings

The administration settings page provides options for configuring global settings for administrator access on the FortiManager device, including:

- Ports for HTTPS and HTTP administrative access

  In order 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, Telnet, 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.
- Language of the GUI

  The default language of the GUI is English. For best results, you should select the language that is used by the management computer.
- Theme of the GUI

  The default color theme of the GUI is *Blueberry*. You can choose another color or an image.
- Password Policy

  The FortiManager unit includes the ability to enforce a password policy for administrator login. With this policy, you can enforce regular changes and specific criteria for a password.
- Display options for the GUI

  You can select to display or hide various advanced configuration options in the GUI. Only the *admin* administrator can configure these system options, which apply to all administrators logging onto the FortiManager unit.

Configuring global administrative settings

To configure the administrative settings:

1. Go to *System Settings* > *Admin* > *Admin Settings*.
2. Configure the following information:

Administration Settings		
	HTTP Port	Type the TCP port to be used for administrative HTTP access. Select to redirect to HTTPS. Default port: 80
	HTTPS Port	Type the TCP port to be used for administrative HTTPS access. Default port: 443
	HTTPS & Web Service Server Certificate	Select a certificate from the drop-down list.
	Idle Timeout	Type the number of minutes that an administrative connection can be idle before the administrator must log in again. The maximum is 480 minutes (8 hours). To ensure security, the idle timeout should be a short period of time to avoid the administrator inadvertently leaving the management computer logged in to the FortiManager unit and opening the possibility of someone walking up and modifying the network options. Range: 1 to 480 (minutes)
View Settings		
	Language	Select a language from the drop-down list.
	Theme	Select a color theme for the GUI. The selected theme is applied when you click *Apply*. Before you click *Apply*, you can try different color themes by clicking each theme.
Password Policy		Select to enable administrator passwords.
	Minimum Length	Select the minimum length for a password. The default is eight characters. Range: 8 to 32 (characters)
	Must Contain	Select the types of characters that a password must contain. Select from the following options: • Upper Case Letters • Lower Case Letters • Numbers (0-9) • Special Characters
	Admin Password Expires after	Select the number of days that a password is valid for, after which time it must be changed.

Display Options on GUI	Select the required options from the list.
Show Script	Select to display the *Script* menu item. This menu is located in the *Device Manager* tab under *Devices & Groups* in the left-hand tree menu. This is an advanced FortiManager feature.
Show Device List Import/Export	Select to display the *Import Device List* and *Export Device List* buttons. These buttons are located in the *Device Manager* tab in the toolbar. This is an advanced FortiManager feature.
Show Add Multiple Button	Select to display the *Add Multiple* button. This button is located in the *Device Manager* tab in the toolbar. This is an advanced FortiManager feature.

3. Select *Apply* to save your settings to all administrator accounts.

Changing the GUI language

The GUI supports multiple languages; the default language is English. You can change the GUI to display in English, Simplified Chinese, Traditional Chinese, Japanese, or Korean. For best results, you should select the language that the management computer operating system uses. You can also set the FortiManager GUI to automatically detect the system language, and by default show the screens in the proper language, if available.

To change the GUI language:

1. Go to *System Settings* > *Admin* > *Admin Settings*.
2. In the *Language* field, select a language from the drop-down list, or select *Auto Detect* to use the same language as configured for your web browser.
3. Select *OK*.

Changing the GUI idle timeout

By default, the GUI disconnects administrative sessions if no activity takes place for five minutes. This idle timeout is recommended to prevent someone from using the GUI from a PC that is logged into the GUI and then left unattended.

To change the GUI idle timeout:

1. Go to *System Settings* > *Admin* > *Admin Settings*.
2. Change the *Idle Timeout* minutes as required (1-480 minutes).
3. Select *Apply*.

Administrator password retries and lockout duration

By default, the number password retries is set to three, allowing the administrator a maximum of three attempts to log into their account before they are locked out for a set amount of time (by default, 60 seconds).

The number of attempts can be set to an alternate value, as well as the default wait time before the administrator can try to enter a password again. You can also change this to further deter would-be hackers. Both settings are must be configured with the CLI.

To configure the lockout options:

```
config system global
   set admin-lockout-duration <seconds>
   set admin-lockout-threshold <failed_attempts>
end
```

For example, to set the lockout threshold to one attempt and a five minute duration before the administrator can try again to log in enter the commands:

```
config system global
   set admin-lockout-duration 300
   set admin-lockout-threshold 1
end
```

Two-factor authentication for administrator log on

To configure two-factor authentication for administrator log on you will need the following:

- FortiManager
- FortiAuthenticator
- FortiToken

Configuring FortiAuthenticator

Before proceeding, ensure that you have configured your FortiAuthenticator and that you have created a NAS entry for your FortiManager and created/imported FortiTokens. For more information, see the *FortiAuthenticator Interoperability Guide* and *FortiAuthenticator Administration Guide* available in the Fortinet Document Library.

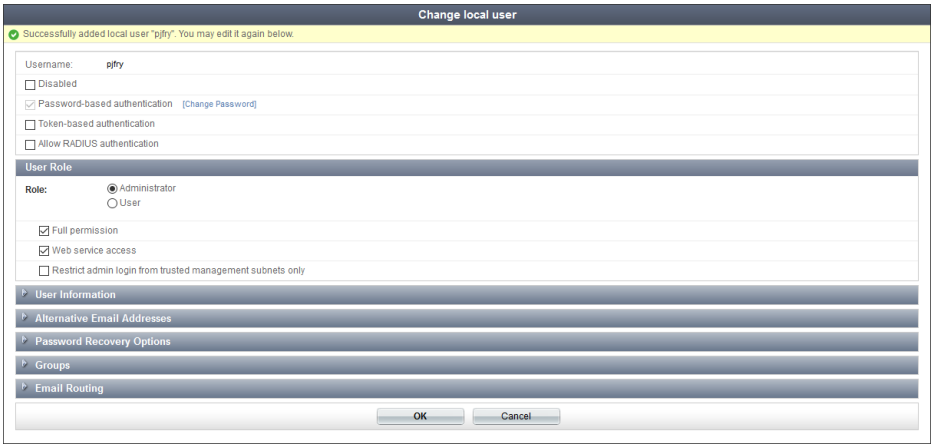
Create a local user:

1. Go to *Authentication* > *User Management* > *Local Users*.
2. Select *Create New* from the toolbar.
3. Configure the following settings:

Username	Type a user name for the local user.
Password creation	Select Specify a password from the drop-down list.
Password	Type a password. The password must be a minimum of 8 characters.
Password confirmation	Re-enter the password. The passwords must match.
Allow RADIUS authentication	Enable to allow RADIUS authentication.
Role	Select the role for the new user.

Enable account expiration	Optionally, select to enable account expiration. For more information see the *FortiAuthenticator Administration Guide*.

4. Select *OK* to continue.



5. Configure the following settings:

Disabled	Select to disable the local user.
Password-based authentication	Leave this option selected. Select *[Change Password]* to change the password for this local user.
Token-based authentication	Select to enable token-based authentication.
Deliver token code by	Select to deliver token by FortiToken, Email or SMS. Select *Test Token* to test the token.
Allow RADIUS authentication	Select to allow RADIUS authentication.
Enable account expiration	Optionally, select to enable account expiration. For more information see the *FortiAuthenticator Administration Guide*.
User Role	
Role	Select either *Administrator* or *User*.
Full Permission	Select to allow Full Permission, otherwise select the admin profiles to apply to the user. This option is only available when *Role* is *Administrator*.
Web service	Select to allow Web service, which allows the administrator to access the web service via a REST API or by using a client application. This option is only available when *Role* is *Administrator*.

	Restrict admin login from trusted management subnets only	Select to restrict admin login from trusted management subnets only, then enter the trusted subnets in the table. This option is only available when *Role* is *Administrator*.
	Allow LDAP Browsing	Select to allow LDAP browsing. This option is only available when *Role* is *User*.

6. Select *OK* to save the setting.

Create a RADIUS client:

1. Go to *Authentication* > *RADIUS Service* > *Clients*.
2. Select *Create New* from the toolbar.
3. Configure the following settings:

For more information, see the *FortiAuthenticator Administration Guide*, available in the Fortinet Document Library.

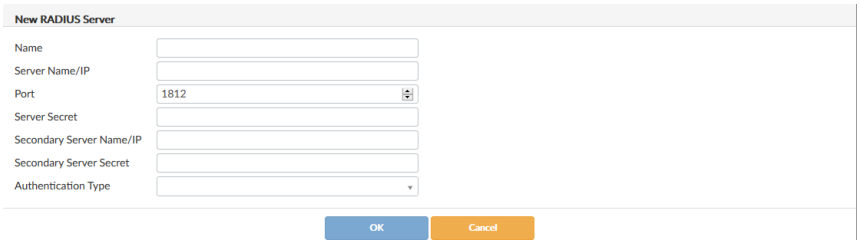
Name	Type a name for the RADIUS client entry.
Client name/IP	Type the IP address or Fully Qualified Domain Name (FQDN) of the FortiManager.
Secret	Type the server secret. This value must match the FortiManager RADIUS server setting at *System Settings* > *Admin* > *Remote Auth Server*.
First profile name	See the *FortiAuthenticator Administration Guide*.
Description	Type an optional description for the RADIUS client entry.
Apply this profile based on RADIUS attributes	Select to apply the profile based on RADIUS attributes.
Authentication method	Select *Enforce two-factor authentication* from the list of options.
Username input format	Select specific user name input formats.
Realms	Configure realms.
Allow MAC-based authentication	Optional configuration.
Check machine authentication	Select to check machine based authentication and apply groups based on the success or failure of the authentication.
Enable captive portal	Enable various portals.
EAP types	Optional configuration.

4. Select *OK* to save the setting.

Configuring FortiManager

To Configure the RADIUS server:

1. Go to *System Settings* > *Admin* > *Remote Auth Server*.
2. Select *Create New* > *RADIUS* from the toolbar.



3. Configure the following settings:

Name	Type a name to identify the FortiAuthenticator.
Server Name/IP	Type the IP address or fully qualified domain name of your FortiAuthenticator.
Server Secret	Type the FortiAuthenticator secret.
Secondary Server Name/IP	Type the IP address or fully qualified domain name of the secondary FortiAuthenticator, if applicable.
Secondary Server Secret	Type the secondary FortiAuthenticator secret, if applicable.
Port	Type the port for FortiAuthenticator traffic.
Authentication Type	Select the authentication type the FortiAuthenticator requires. The default setting of *ANY* has the FortiManager unit try all the authentication types.

4. Select *OK* to save the setting.

To create the administrator users:

1. Go to *System Settings* > *Admin* > *Administrator.*
2. Select *Create New* from the toolbar.
3. Configure the settings, selecting the previously added RADIUS server from the *RADIUS Server* drop-down list. See Configuring RADIUS administrator accounts on page 69.
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 select *Login*.
3. Enter your FortiToken pin code and select *Submit* to log in to FortiManager.

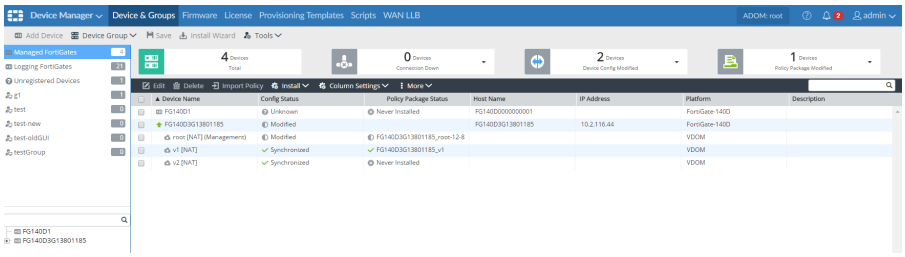
Device Manager

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

This chapter 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 56.



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

Devices & 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 95. The *Device & Groups* tab also contains a quick status bar for a selected device group. See Using the quick status bar on page 120.
Firmware	View information about firmware for devices as well as upgrade firmware. See Firmware on page 133.
License	View license information for devices as well as push license updates to devices. See License on page 135.
Provisioning Templates	Configure provisioning templates. For information on system, Threat Weight, FortiClient, and certificate templates, see Provisioning Templates on page 137.
Scripts	Create new or import scripts. Scripts is disabled by default. You can enable this advanced configuration option in *System Systems* > *Admin* > *Admin Settings*. Select *Show Script* to enable on this option in the *Device Manager* pane. See Scripts on page 143.

WAN LLB	Configure profiles for load balancing WAN links and monitor load-balancing profiles. The *WAN LLB* tab is displayed only when central WAN Link load balancing is enabled. See WAN Link Load Balance on page 173.
FortiExtender	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 5.4 devices into one ADOM, and all 5.2 devices into another.
- Geographic regions: group all devices for a specific geographic region into an ADOM, and devices for a separate region into another ADOM.
- Administrator users: group devices into separate ADOMs based for specific administrators responsible for the group of devices.
- Customers: group all devices for one customer into an ADOM, and devices for another customer into another ADOM.

  FortiAnalyzer, FortiCache, FortiClient, FortiDDos, FortiMail, FortiManager, FortiSandbox, FortiWeb, Chassis, and FortiCarrier devices are automatically placed in their own ADOMs.

Each administrator profile can be customized to provide read-only, read/write, or restrict access to various ADOM settings. When creating new administrator accounts, you can restrict which ADOMs the administrator can access, for enhanced control of your administrator users. For more information on ADOM configuration and settings, see Administrative Domains on page 49 .

For information on adding devices to an ADOM by using the *Add Device* wizard, see Adding devices with the wizard on page 96.

Adding devices

You must add devices to the FortiManager system to use FortiManager to manage or receive logs from the devices. You must also enable central management or logging on the device that will be connected to the FortiManager. 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. When adding devices by using the *Add Device* wizard, you have more configuration options than when you use the *Add Multiple* option.

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 will 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, but select *Add Model Device* instead of *Discover*.

Adding an operating FortiGate HA cluster to the *Device Manager* pane is similar to adding a standalone device. Type the IP address of the master device, the FortiManager handles a cluster as a single managed device.

Adding devices with 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.

Use the *Discover* option for devices that are currently online and discoverable on your network.

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

When configuring a model device to automatically promote or register 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 <FMGSN> <KEY>` command from the FortiGate console. The device is automatically promoted or registered, 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 <FMGSN> <KEY> <username> <password>` command.

Use the fast forward support feature to ignore prompts when adding or importing a device. The wizard will only stop if there are errors with adding a device or importing policies or objects from a device or VDOM.

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
```

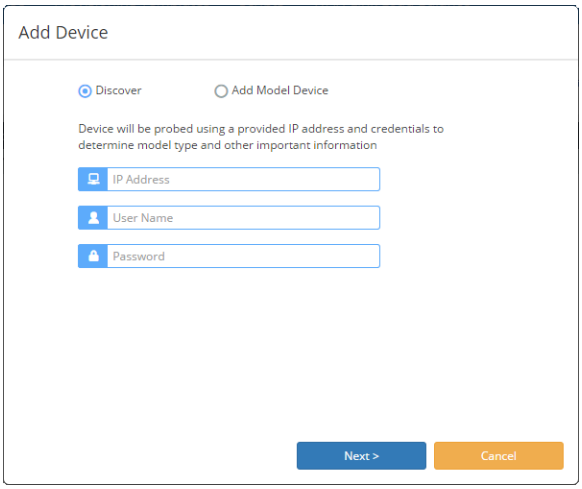
Add a device using discover mode

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

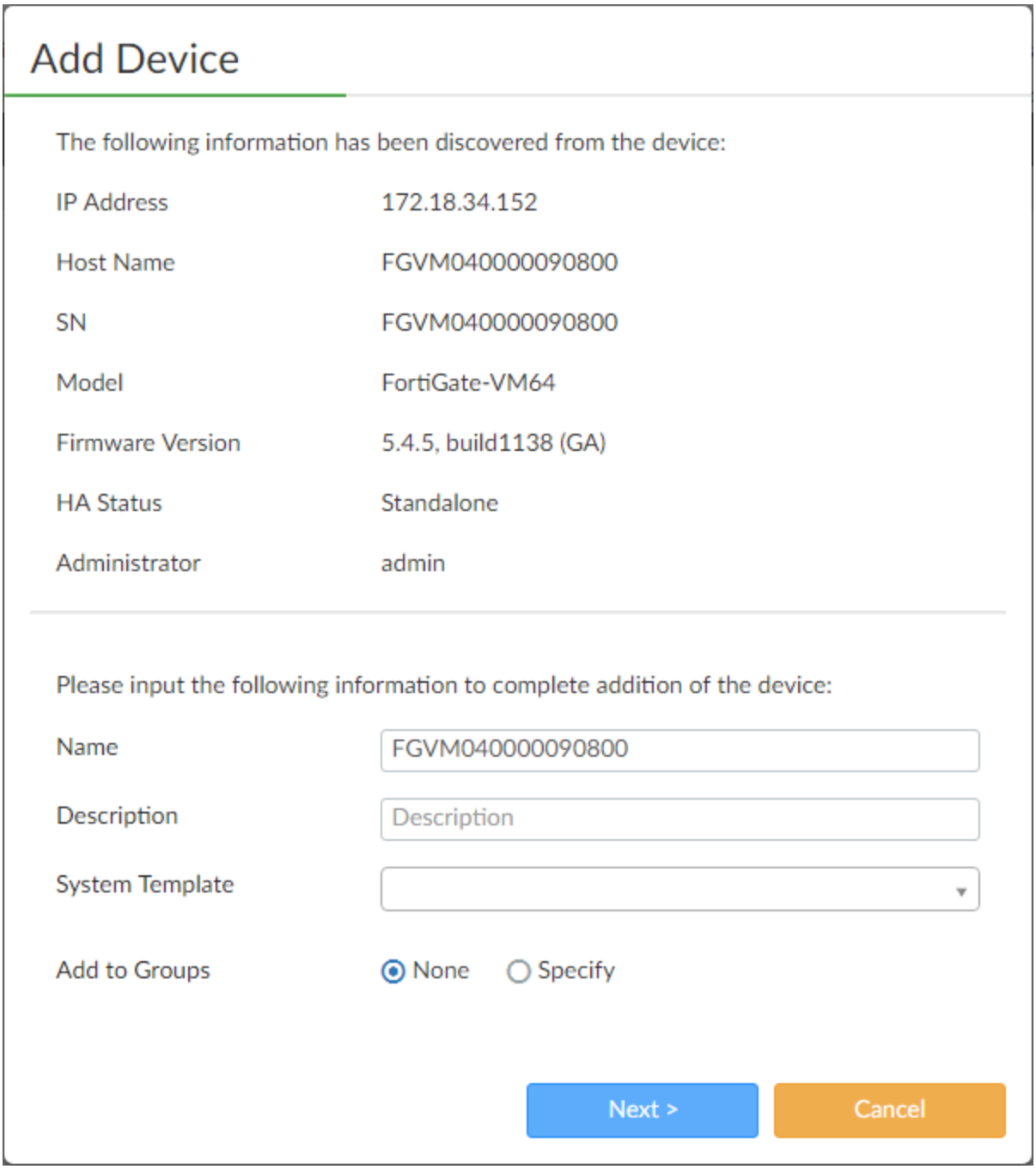
FortiManager will not be able to communicate with the FortiGate if offline mode is enabled. Enabling offline mode will prevent FortiManager from discovering devices.

To add a device using discover mode:

1. If 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 wizard opens.



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 (build)
   - High Availability mode
   - Administrator user name



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. f required, assign a system template using the drop-down menu. Alternatively, you can select to configure all settings per-device inside *Device Manager*. For more information, see Provisioning Templates on page 137.
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
   - Retrieving high availability status
   - Initializing configuration database
   - Retrieving interface information
   - Retrieving configuration
   - Loading to database
   - Creating initial configuration file
   - Retrieving IPS signature information
   - Retrieving support data
   - Updating group membership
   - Successfully add device
   - Check device status
7. Choose whether to import policies and objects for the device now or later. For now, click *Import Now*; for later, click *Import Later*.
8. Select *Next* to continue.
9. System templates can be used to centrally manage certain device-level options from a central location.
   If required, assign a system template using the drop-down menu. Alternatively, you can select to configure all settings per-device inside *Device Manager*. For more information, see Provisioning Templates on page 137.
10. Select *Next* to continue.
    If VDOMs are not enabled on the device, the wizard will skip the VDOM phase. You can Select to import each VDOM step by step, one at a time, or automatically import all VDOMs.

    The following import options are available:

Import Options	The wizard will detect if the device contains virtual domains (VDOMs). You can select the behavior for FortiManager to take to import these VDOMs. Import options include: • *Import each VDOM step by step* • *Import VDOM one at a time* • *Automatically import all VDOMs*

11. Select *Next* to complete the VDOM import.
    When selecting to import the VDOM step-by-step or one of the time, you can use the global zone map section of the wizard to map your dynamic interface zones.

12. Select *Next* to continue to interface mapping.

When importing configurations from a device, all enabled interfaces require a mapping.

13. Map all the enabled interfaces to ADOM level interfaces.
14. If required, select *Add mappings for all unused device interfaces*, than select *Next* to continue.
15. The wizard will perform a policy search in preparation for importing them into FortiManager's database. When complete, a summary of the policies will be shown.

    Choose a folder from the drop-down list, type a new policy package name, and select the policies and objects that need to be imported.
16. Select *Next* to continue. The wizard searches the unit for objects to import, and reports any conflicts it detects. If conflicts are detected, you must decide whether to use the FortiGate value or the FortiManager value.

    If there are conflicts, you can select *View Details* to view details of each individual conflict, or you can download an HTML conflict file to view all the details about the conflicts.
17. Select *Next*. The objects that are ready to be imported are shown.
18. Select *Next* to import policies and objects into the database.
19. Select *Next*.

    A detailed summary of the import is shown, and the Import Report can be downloaded. This report is only available on this page.
20. Click *Finish* to close the wizard.

Add a model device

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

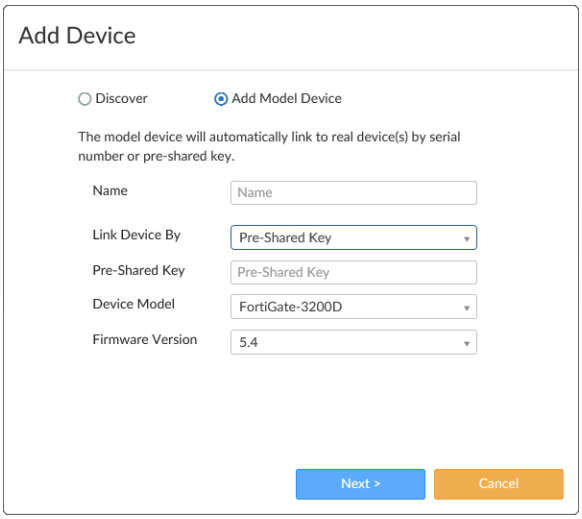
To confirm that a device model or firmware version is supported by the FortiManager's current firmware version, run the following CLI command:

```
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 is displayed.



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

Add Model Device	Device will be added using the chosen model type and other explicitly entered information.
Name	Type a descriptive name for the device. This name is displayed in the *Device Name* column. Each device must have a unique name. Otherwise the wizard will fail.
Link Device By	The method by which the device will be added, either *Serial Number* or *Pre-Shared Key*.
Serial Number or Pre-Shared Key	Type the device serial number or pre-shared key. This field is mandatory.
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.
Firmware Version	Select the device's firmware version from the drop-down list.

5. Select *Next* to continue. The device will be created in the FortiManager database.

Each device must have a unique name and pre-shared key (if selected), otherwise the wizard will fail.

6. Click *Finish* to exit the wizard.

   A device added using the *Add Model Device* wizard has similar dashboard options as a device which is added using the *Discover* option. As the device is not yet online, some options are not available.

The pre-shared key can be edited after the model device has been added (see Editing device information on page 121), but must always be unique.

Adding devices manually

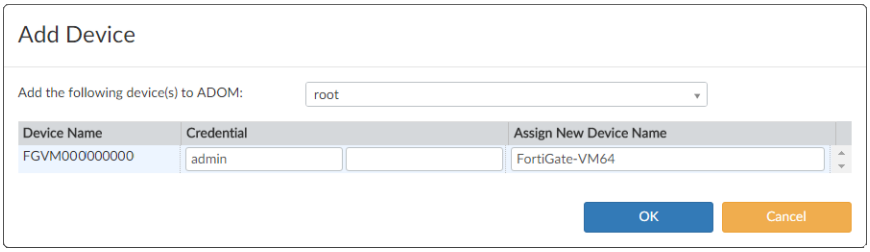
You can manually add devices to the FortiManager unit. The process requires the following steps:

- You must enable central management on the device by adding the IP address of the FortiManager unit. The device will be listed on the FortiManager GUI in the root ADOM on the *Device Manager* pane in the *Unregistered Devices* list.
- In FortiManager, you must manually add unregistered devices. The device will be registered with the FortiManager unit, and you can use FortiManager to manage the device.

When ADOMs are enabled, the device must be assigned to an ADOM when it is registered. Non FortiGate devices are assigned to their respective device specific ADOMs.

To manually add devices:

1. On the device, enable central management or central logging, depending on the device type.
2. In FortiManager, select the root ADOM, and go to *Device Manager*.
3. In the tree menu, click *Unregistered Devices*. The content pane displays the unregistered devices.
4. Select the unregistered device or devices, then click *Add*. The *Add Device* dialog box opens.



5. If ADOMs are enabled, select the ADOM in the *Add the following device(s) to ADOM* list. If ADOMs are disabled, select *root*. Non FortiGate devices are added to their respective device specific ADOMs.
6. Type the log in and password for the device or devices.
7. Click *OK* to register the device or devices.

   The device or devices are added.

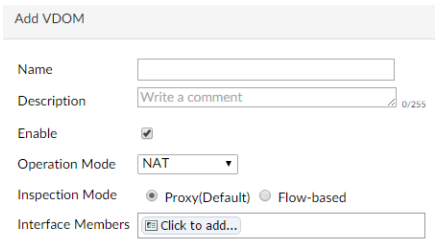
Add a VDOM to a device

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.

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.

To add a 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. Configure the following options, and click *OK*.

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 *NAT* or *Transparent*.
Inspection Mode	Select an inspection mode.
Interface Members	Click to select each port one by one.

Import policy wizard

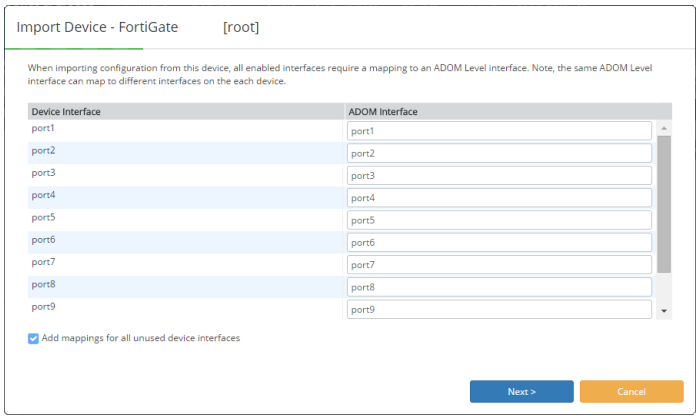
On the *Device Manager* > *Device & Groups* pane, right-click a device, and select *Import Policy* to launch the *Import Device* wizard. This wizard will allow you to import interface maps, policy databases, and objects.

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.

Device Interface

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

Interface maps will be created automatically for unmapped interfaces.



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

Policy

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

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

Policy Package Name	Type a name for the policy package.
Folder	Select a folder on the drop-down menu.
Policy Selection	Select to import all, or select specific policies and policies groups to import.
Object Selection	Select *Import only policy dependent objects* to import policy dependent objects only for the device. Select *Import all objects* to import all objects for the selected device.

Object

The object page will search for dependencies, and reports any conflicts it detects.If conflicts are detected, you must decide whether to use the FortiGate value or the FortiManager value. If there are conflicts, you can select *View Details* to view details of each individual conflict, or you can download an HTML conflict file to view all the details about the conflicts. Duplicates will not be imported.

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

Import

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

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

Summary

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

Importing devices

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 *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

You can import or export large numbers of devices, ADOMs, device VDOMs, and device groups, using the *Import Device List* and *Export Device List* toolbar buttons. The device list is a compressed text file in 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* check box 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.

You can create the compressed text file by exporting a device list from FortiManager.

To export a device list:

1. Go to *Device Manager* > *Device & Groups*.
2. Select a device group, such as *Managed FortiGates*.
3. From the *More* menu, select *Export Device List*.
   A device list in JSON format is exported in a compressed file (`device_list.dat`).

To import a device list:

1. Go to *Device Manager* > *Device & Groups*.
2. Select a device group, such as *Managed FortiGates*.
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.
5. Click *OK* .

Configuring devices

You can configure the FortiGate units in three ways:

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

This section contains the following topics:

Configuring a device

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 *RevisionHistory* window.

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 353.

Configuring VDOMs

Virtual domains (VDOMs) enable you to partition and use your FortiGate unit as if it were multiple units. For more information see the FortiOS Handbook available in the Fortinet Document Library.

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 *Apply* .

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, SNMP, and/or TELNET.
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 110 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.

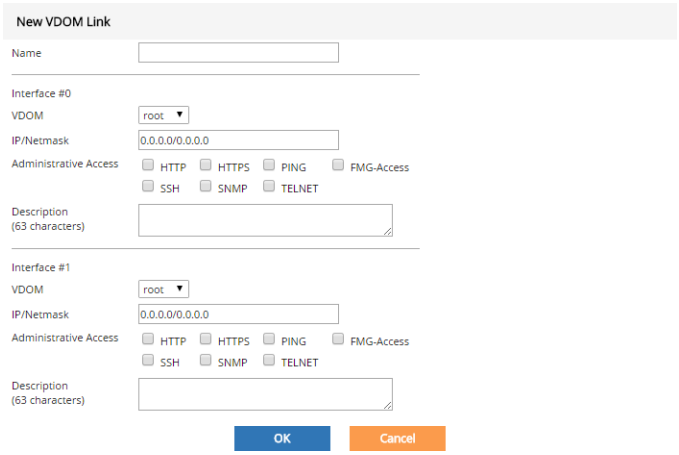
Before configuring inter-VDOM routing:

- 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 virtual domain.
2. From the *System* menu, select *Interface* .
3. Click *Create New* > *VDOM Link* . The *New VDOM Link* pane opens.



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 from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, and Web Service.
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 193). 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

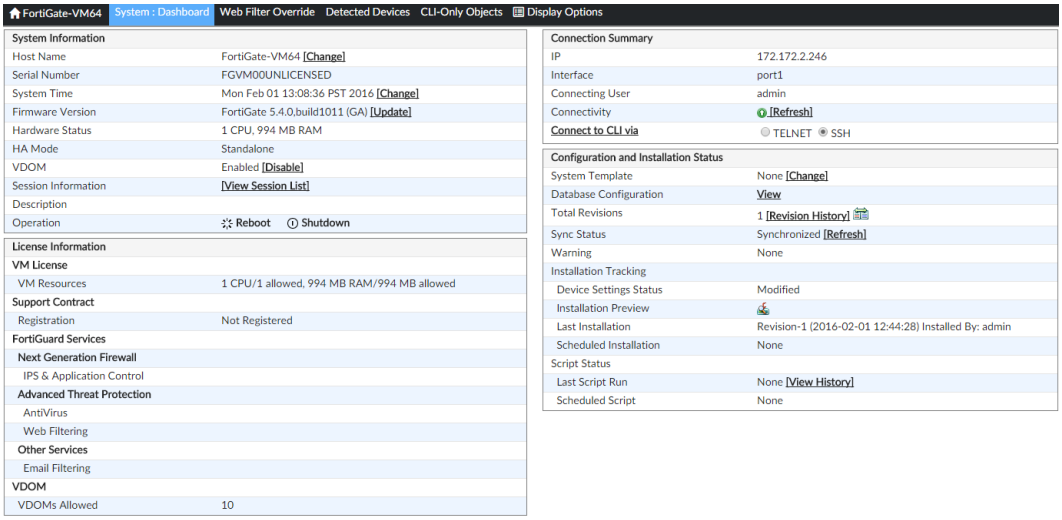
You can view information about individual devices in the *Device Manager* pane on the dashboard for each device. This section describes the dashboard for a FortiGate unit.

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 FortiGates*. 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 FortiGates* and *Logging FortiGates*. Managed FortiGates include FortiGate devices, which are managed by FortiManager but do not send logs. Logging FortiGates 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 111.

   For information on configuring FortiGate settings locally on your FortiManager device, see the *FortiOS Handbook*.

5. You can control what tabs are displayed by clicking *Display Options*. See Display Options on page 111.

Dashboard toolbar

The dashboard toolbar displays a number of tabs that you can use to configure the device. The available tabs are dependent on the device. You can also choose what tabs are displayed by using the display options.

The options available on the dashboard toolbar will vary from device to device depending on what feature set the device supports. If a feature is not enabled on the device the corresponding tab will not be available on the toolbar.

Display Options

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

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 check box beside the category name. To reset a category selection, clear the check box.

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 FortiGates*. 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. The following options are available:

Create New	Select to create a new interface or a VDOM link.
Edit Interface Map	Edit the selected interface.
Collapse All / Expand All	Click to collapse or expand all interfaces.
Interface	Name of the interface.
Type	Type of interface.
Mapped Policy Interface	Name of the policy, if the interface is mapped to a policy.
Addressing Mode	Type of addressing mode, either manual or DHCP.
IP/Netmask	IP address and netmask for the interface.
Access	Configured access to the interface.
Virtual Domain	Name of the virtual domain.
Status	Status of the interface. A green circle indicates that the interface is online, and a red circle indicates that the interface is offline.

CLI-Only Objects menu

FortiManager includes a *CLI-Only Objects* menu in the *Device Manager* pane, which allows you to configure device settings that are normally configured via the CLI on the device.

To access the CLI-only objects menu:

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

The options available in the menu will vary from device to device depending on what feature set the device supports. The options will also vary depending on the device firmware version. This menu includes CLI commands which are only available in the CLI.

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 5.0:

- 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.

System Information	
Host Name	The host name of the device.
Serial Number	The device serial number.
System Time	The device system time and date information.
Firmware Version	The device firmware version and build number.
Hardware Status	The number of CPUs and the amount of RAM for the device.
HA Mode	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.
VDOM	The status of VDOMs on the device.
Session Information	Select *View Session List* to view the device session information.
Description	Descriptive information about the device.
Operation	Select *Reboot* to reboot the device or *Shutdown* to shut down the device.

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.

Connection Summary	
Interface	The port used to connect to the FortiManager system.
Connecting User	The user name for logging in to the device.
Connectivity	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. Select *Refresh* to test the connection between the device and the FortiManager system.
Connect to CLI via	Select the method by which you connect to the device CLI, either SSH or TELNET.

Configuration and Installation Status	
System Template	The system template associated with the device. Select *Change* to set this value.
Database Configuration	Select *View* to display the configuration file of the FortiGate unit.
Total Revisions	Displays the total number of configuration revisions and the revision history. Select *Revision History* to view device history. Select the revision history icon to open the *Revision Diff* menu. You can view the diff from a previous revision or a specific revision and select the output.
Sync Status	The synchronization status with the FortiManager. • *Synchronized*: The latest revision is confirmed as running on the device. • *Out_of_sync*: The configuration file on the device is not synchronized with the FortiManager system. • *Unknown*: The FortiManager system is unable to detect which revision (in revision history) is currently running on the device. Select *Refresh* to update the Installation Status.
Warning	Displays any warnings related to configuration and installation status. • *None*: No warning. • *Unknown configuration version running on FortiGate: FortiGate configuration has been changed!*: The FortiManager system cannot detect which revision (in *Revision History*) is currently running on the device. • *Unable to detect the FortiGate version*: Connectivity error! • *Aborted*: The FortiManager system cannot access the device.
Installation Tracking	

Configuration and Installation Status		
	Device Settings Status	• *Modified*: Some configuration on the device has changed since the latest revision in the FortiManager database. Select *Save Now* to install and save the configuration. • *UnModified*: All configuration displayed on the device is saved as the latest revision in the FortiManager database.
	Installation Preview	Select the icon to display a set of commands that will be used in an actual device configuration installation in a new window.
	Last Installation	*Last Installation*: The FortiManager system sent a configuration to the device at the time and date listed.
	Scheduled Installation	*Scheduled Installation*: A new configuration will be installed on the device at the date and time indicated.
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.

Installing to devices

This section includes the following topics:

Install policy package and device settings

You can install policy package and device settings using the *Install* wizard.

To import policies to a device:

1. Click *Install Wizard* in the toolbar. The *Install Wizard* will appear.
2. Select *Install Policy Packages & Device Settings* .
   This option will install a selected policy package to the device. Any device specific settings for devices associated with the policy package will also be installed.
3. Follow the steps in the wizard to install the policy package to the device.

For information on importing policy packages and device settings to a device using the *Install* wizard, see Install wizard on page 116.

Install wizard

The Install wizard assists you in installing policy packages and device settings to one or more FortiGate devices.

Launching the install wizard

To launch the *Install* wizard, select the *Install Wizard* or *Install* icon in the toolbar.

The *What to Install* page provides the following options:

- Install policy package and device settings on page 115: Install a selected policy package. Any device specific settings for devices associated with package will also be included.
- Install device settings (only) on page 117: Install only device settings for a select set of devices. Policy and object changes will not be updated from the last install. This option is only available when launching the *Install Wizard* in the Device Manager tab.
- Install interface policy (only) on page 118: Install interface policy only in a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Install policy package and device settings

1. Select *Install Policy Package & Device Settings*.
2. Configure the following options:

Policy Package	Select the policy package from the drop-down list.
Comment	Type an optional comment.
Create Revision	Select the check box to create a revision.
Revision Name	Type the revision name.
Revision Comments	Type an optional comment.
Schedule Install	Select the check box 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 drop-down lists.

3. Select *Next* to continue.

Device selection

The device selection page allows you to choose one or more devices or groups to install. Select the required devices or groups, then select *Next* to continue.

Validation

The *Validation* page checks the following:

- *Installation Preparation*
- *Interface Validation*
- *Policy and Object Validation*
- *Ready to Install Policy Package*, or *Ready to Install (date time)* when *Schedule Install* is selected

Devices with a validation error will be skipped for installation.

The following options are available:

Preview	Select to view device preview.
Download	Select download to open or save the preview file in `.txt` format.
Install/Schedule Install	Select to proceed to the next step in the install wizard.

The last page of the a scheduled install is the Summary page. Otherwise the last page is the installation page.

Installation

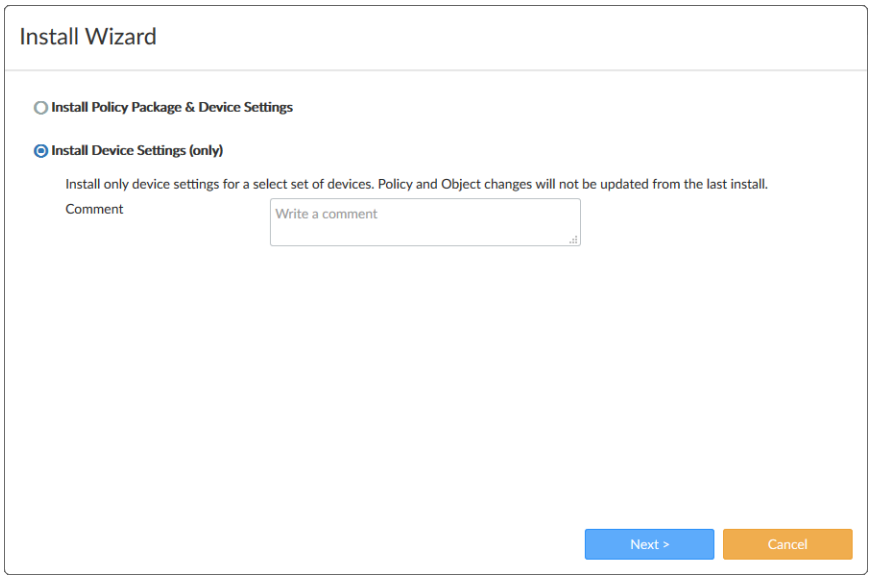
The installation phase displays the status of the installation process, and then lists the devices onto which the settings were installed and any errors or warning that occurred during the installation process.

Selecting the history icon for a specific device will open the installation history for that device.

Install device settings (only)

Select *Install Device Settings (only)* and optionally, type a comment for the device settings being installed.

This option is only available when launching the *Install Wizard* in the *Device Manager* tab.



Device selection

The device selection window allows you to choose the device type, then one or more devices of that type to install. Select devices, then select *Next* to continue.

Validation

Validation performs a check on the device and settings to be installed. Select *Preview* to preview the installation, or select *Download* to open or save the preview file in `.txt` format, then select *Next* to continue.

Installation

The installation window displays the status of the installation process, and then lists the devices onto which the settings were installed and any errors or warning that occurred during the installation process.

Selecting the history icon for a specific device will open the installation history for that device.

Install interface policy (only)

Select *Install Interface Policy (only)*, then select a policy package. Optionally, type a comment for the interface policy being installed. Select *Next* to continue.

Device selection

The device selection window allows you to choose the device type, then one or more devices of that type to install. Select devices, then select *Next* to continue.

Validation

The validation phase will perform a check on the device and settings to be installed. Select *Preview* to preview installation, or select *Download* to open or save the preview file in `.txt` format, then select *Next* to continue.

Installation

The installation window displays the status of the installation process, and then lists the devices onto which the settings were installed and any errors or warning that occurred during the installation process.

Selecting the history icon for a specific device will open the installation history for that device.

Re-install Policy

You can right-click on the device row and select *Re-install Policy* to perform a quick install of a policy package without launching the *Install Wizard*. The content menu is disabled when the policy package is already synchronized. You can also right-click on the configuration status if the device is out of synchronization to install any device setting changes. This will only affect the settings for the selected device.

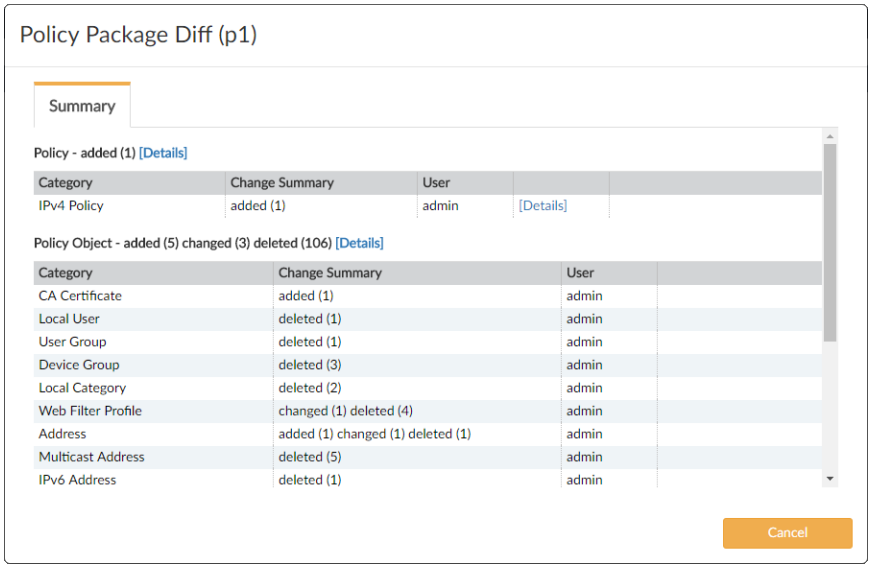
View a policy package diff

You can view the difference between the current policy package and the policy in the device by using *Device Manager*.

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. Go to *Device Manager> Device & Groups*.
2. Right-click a device and select *Policy Package Diff*.
   The *Policy Package Diff* window is displayed after data is gathered.



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

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 also 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. 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.

You can also filter columns that have a Filter icon..

The columns displayed will vary by device type. Column settings or not available for all device types. Column filters are not available for all columns.

The columns available in Column Settings is dependent 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 the *Column Settings* menu, and select the columns that 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. From the *More* menu, select *Refresh*. The *Update Device* dialog box opens to show the refresh progress.

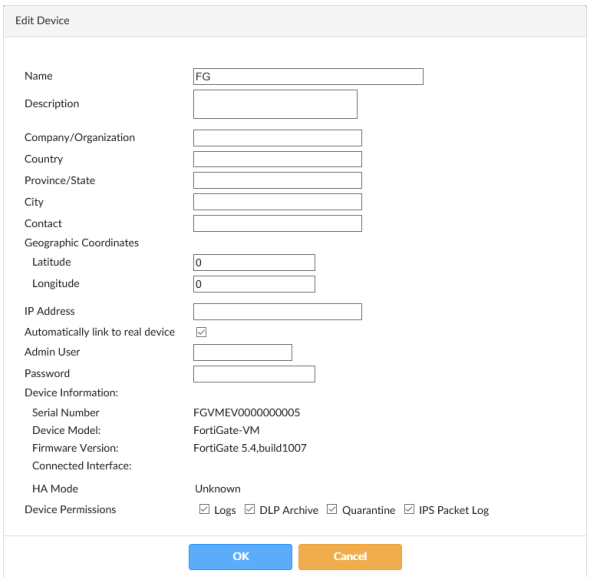
Editing device information

Device and model device information can be edited.

The information and options available in the *Edit Device* page is dependent on the device type and firmware version.

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*. The *Edit Device* pane is displayed.



4. Edit the following settings as required.

Name	The name of the device.
Description	Descriptive information about the device.
Company /Organization	Company or organization information.
Country	Type the country.
Province/State	Type the province or state.
City	Type the city.
Contact	Type the contact name.
Geographic coordinates	Identifies the latitude and longitude of the device location to support the interactive map available with FortiView when the FortiAnalyzer features are enabled.
IP Address	The IP address of the device.
Pre-shared Key	The model device's pre-shared key. Select *Show Pre-shared Key* to see the key. This option is only available when editing a model device that was added with a pre-shared key.
Automatically link to real device	Automatically register the device with FortiManager when the device is online.
Admin User	The administrator user name.
Password	The administrator user password

Device Information	Information about the device, including some or all of: serial number, device model, firmware version, connected interface, HA mode, cluster name, and cluster members.
Device Permissions	Specify the permissions for the FortiGate device. Select *Logs*, *DLP Archive*, *Quarantine*, or *IPS Packet Log*.

The available options are dependent on the features enabled. Some settings will only be displayed when the FortiAnalyzer Feature set is enabled.

5. After making the appropriate changes click *OK*.

Enable *Secure Connection* to secure OFTP traffic over IPsec. When enabling *Secure Connection*, load on the FortiManager is also increased. This feature is disabled by default.

In an HA environment, if you enable *Secure Connection* on one cluster member, you need to enable *Secure Connection* on the other cluster members.

Replacing a managed device

The serial number will be verified before each management connection. In the event of a replaced device, it is necessary to 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 being 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 unregistered device options

In 5.2, setting unregistered device options is from the CLI only. Type the following command lines to enable or disable allowing unregistered devices to be registered with the FortiManager.

```
config system admin setting
   (setting) set allow register [enable | disable]
   (setting) set unreg_dev_opt add_allow_service
   (setting) set unreg_dev_opt add_no_service
end
```

allow register [enable | disable]	When the set allow register command is set to enable, you will not receive the following unregistered device dialog box.
unreg_dev_opt	Set the action to take when an unregistered device connects to the FortiManager.
add_allow_service	Add unregistered devices and allow service requests.
add_no_service	Add unregistered devices but deny service requests.

When the `set allow register` command is set to `disable`, you will not receive the unregistered 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 is displayed.
3. On the *Connection Summary* widget, choose either TELNET or SSH, and click *Connect to CLI via*.

Connect to:	Shows the device that you are currently connected to. Select the drop-down menu to select another device.
IP	The IP address of the connected device.
Telnet | SSH	Connect to the device via Telnet or SSH.
Connect | Disconnect	Connect to the device you select, or terminate the connection.
Close	Exit the CLI console.

You can cut (Control key + C) and paste (Control key + V) text from the CLI console. You can also use Control key + U to remove the line you are currently typing before pressing *ENTER*.

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

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 FortiGates*. 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	Name of the device
Config Status	See the table below for config status details.
Policy Package Status	See the table below for policy package status details.
Hostname	Available for managed devices. Displays the host name for the device.
IP Address	IP address of the device
Platform	Available for managed devices. Displays the platform of the device.
Logs	Available for logging devices. Identifies whether logs are being sent from the managed device to FortiManager. Red indicates that no logs are being sent, and green indicates that logs are being sent. A lock icon indicates a secure connection.
Average Log Rate (log/sec)	Available for logging devices. Displays the average rate of logs being sent from the managed device to FortiManager.
Device Storage	Available for logging devices. Displays how much of the available disk space for the device is consumed by logs.
Description	Description of the device

The following table identifies the different available config statuses.

Config Status	Icon	Description
Synchronized	Green check	Configurations are synchronized between FortiManager and the managed device.
Modified	Yellow triangle	Configurations are modified on FortiManager and not synchronized between FortiManager and the managed device.
Auto-update	Green check	Configurations modified on the managed device are auto synced to FortiManager.
Modified (recent auto-updated)	Yellow triangle	Configurations are modified on FortiManager and configurations modified on the managed device are auto synced to FortiManager.
Out of Sync	Red X	Configurations are modified on the managed device and not synced to FortiManager.
Conflict	Red X	When one of the following happens: • Install failed • Configurations are modified on both FortiManager and the managed device, and not auto synced to FortiManager.
Unknown	Gray question mark	When one of the following happens: • Connection goes down • No revision is generated, like added model device

The following table identifies the different available policy package statuses.

Policy Package Status	Icon	Description
Imported	Green check	Policies and objects are imported into FortiManager.
Synchronized	Green check	Policies and objects are synchronized between FortiManager and the managed device.
Modified	Yellow triangle	Policies or objects are modified on FortiManager.
Out of Sync	Red X	Policies or objects are modified on the managed device.
Unknown with policy package name	Gray question mark	Configurations of the managed device are retrieved on FortiManager after being imported/installed.
Never Installed	Yellow triangle	No policy package is imported or installed.

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*.
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. In the dashboard, locate the *Configuration and Installation Status* widget.
   The following information is shown:

System Template	Displays the name of the selected system template. Select *Change* to change the system template.

Database Configuration	Select *View* to display the configuration file of the FortiGate unit.
Total Revisions	Displays the total number of configuration revisions and the revision history. Select *Revision History* to view device history. Select the icon to view the *Revision Diff* dialog box.
Sync Status	The synchronization status with the FortiManager. • *Synchronized*: The latest revision is confirmed as running on the device. • *Out_of_sync*: The configuration file on the device is not synchronized with the FortiManager system. • *Unknown*: The FortiManager system is unable to detect which revision (in revision history) is currently running on the device. Select *Refresh* to update the Installation Status.
Warning	Displays any warnings related to configuration and installation status. • *None*: No warning. • *Unknown configuration version running on FortiGate: FortiGate configuration has been changed!*: The FortiManager system cannot detect which revision (in *Revision History*) is currently running on the device. • *Unable to detect the FortiGate version*: Connectivity error! • *Aborted*: The FortiManager system cannot access the device.
Installation Tracking	
Device Settings Status	• *Modified*: Some configuration on the device has changed since the latest revision in the FortiManager database. Select *Save Now* to install and save the configuration. • *UnModified*: All configuration displayed on the device is saved as the latest revision in the FortiManager database.
Installation Preview	Select 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 time and date listed.
Scheduled Installation	A new configuration will be installed on the device at the date and time indicated.
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.

Managing configuration revision history

In the *Device Manager* > *Device & Groups* pane, select a device group, and then select a device in the lower tree menu. In the device dashboard *Configuration and Installation Status* widget, select *Revision History* in the *Total Revisions* row, to view the FortiManager repository.

The repository stores all configuration revisions for the devices, and tags each revision with a version/ID number. You can view the version history, inspect configuration changes, import files from a local computer, view configuration settings, compare different revisions, revert to previous settings, and download configuration files to a local computer.

The following buttons are displayed 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. See Comparing different configuration files on page 131 for more details.
Retrieve Config	Select to check out 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 will be created and assigned a new ID number.
Download Factory Default	Download the factory default configuration file.
Return	Return to the device dashboard.

The following additional options are available in the right-click menu:

Revert	Revert the current configuration to the selected revision. See To revert to another configuration file: on page 132.
Delete	Delete this version from the repository. You cannot delete a version that is currently active on the FortiGate unit.
Rename	Type a name for the selected revision.
Import Revision	Select to import a configuration file from a local computer to the FortiManager system. See To import a configuration file from a local computer: on page 131.

The following columns of information are displayed:

ID	A number assigned by the FortiManager system to identify the version of the configuration file saved in the FortiManager repository. Select an ID to view the configuration file. You can also select the Download button to save this configuration file from the FortiManager system to a local computer.
Date & Time	The time and date when the configuration file was created.
Name	A name added 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 whether a configuration file has been installed or is currently active. The installation time and date is displayed. N/A status indicates that a particular revision was not sent to the device. The typical situation is that the changes were part of a later revision that was sent out to the device. For example, you make some changes and commit the changes. Now you have a revision called ID1. Then you make more changes and commit the changes again. Then you have a revision called ID2, which also includes the changes you made in revision ID1. If you install revision ID2, then the status of revision ID1 becomes N/A.
Comments	Display the comment added to this configuration file when you edit the file name.

The following procedures assume that you are already viewing the devices' dashboard menus in the right-hand content pane.

To view the configuration settings on a FortiGate unit:

1. Go to *Device Manager* > *Device & Groups* pane, and select a device group.
2. In the lower tree menu, select a device. The device dashboard is displayed.
3. In the *Configuration and Installation Status* widget, in the *Total Revisions* row, select *Revision History*.
4. Select the revision, and click *View Config*. The *View Configuration* pane is displayed.
5. Click *Return* when you finish viewing.

   You can download the configuration settings if you want by selecting *Download* in the *View Configuration* pane.

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

1. Go to *Device Manager* > *Device & Groups* pane, and select a device group.
2. In the lower tree menu, select a device. The device dashboard is displayed.
3. In the *Configuration and Installation Status* widget, in the *Total Revisions* row, select *Revision History*.
4. Right-click the revision, and select *Rename*.
5. Type a name in the *Tag (Name)* field.

6. Optionally, type information in the *Comments* field.
7. Click *OK*.

Downloading and importing a configuration file

You can download a configuration file and a factory default configuration file to a local computer. You can also import the file back to the FortiManager repository.

You can only import a configuration file that is downloaded from the FortiManager repository. Otherwise the import will fail.

To download a configuration file to a local computer:

1. Go to *Device Manager* > *Device & Groups* pane, and select a device group.
2. In the lower tree menu, select a device. The device dashboard is displayed.
3. In the *Configuration and Installation Status* widget, in the *Total Revisions* row, click *Revision History*.
4. Select the revision you want to download.
5. Click *View Config* > *Download*.
6. Select *Regular* or *Encrypted* download type. If you select *Encrypted Download*, type a password.
7. Click *OK*.
8. Specify a location to save the configuration file on the local computer.
9. Click *Save*.

To download a factory default configuration file to a local computer:

1. In the device dashboard, go to the *Configuration and Installation Status* widget, in the *Total Revisions* row, select *Revision History*.
2. Select *Download Factory Default* in the toolbar.

To import a configuration file from a local computer:

1. In the device dashboard, go to the *Configuration and Installation Status* widget, in the *Total Revisions* row, select *Revision History*.
2. Right-click the revision list, and select *Import Revision*.
3. Select *Choose File* to locate the file.
4. If the file is encrypted, select the *File is Encrypted* check box, and type the password.
5. 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 on *Device Manager* pane and select *Commit*, the new configuration file will be 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 the *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 will be shown. This is because version/ID 2 and version/ID 3 have both been sequenced in the same way in the *Device Manager*.

The following procedures assume that you are already viewing the devices' menus in the left-hand pane.

To compare different configuration files:

1. Go to *Device Manager* > *Device & Groups* pane, and select a device group.
2. In the lower tree menu, select a device. The device dashboard is displayed.
3. In the *Configuration and Installation Status* widget, in the *Total Revisions* row, click *Revision History*.
4. Select a revision, and click *Revision Diff* in the toolbar.
5. Select another version for the diff by using the *Select Version* list or by selecting *Factory Default*.
6. Select whether to display the full configuration file (*Full Content*) or only the differences (*Diff Only*) in *Output*. You can also choose to capture the diff to a script.

   The *Full Content* mode shows all configuration settings and highlights all configuration differences while the *Diff Only* mode solely highlights configuration differences.
7. Click *Apply*.

   The configuration differences are displayed in colored highlights:

To revert to another configuration file:

1. Go to *Device Manager* > *Device & Groups* pane, and select a device group.
2. In the lower tree menu, select a device. The device dashboard is displayed.
3. In the *Configuration and Installation Status* widget, in the *Total Revisions* row, click *Revision History*.
4. Right-click the revision to which you want to revert, and click *Revert*.
5. Click *OK*.

   The system 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, the devices are displayed in default groups based on the type of device. For example, all FortiGate devices are displayed in the *Managed FortiGates* group. You can create custom groups as needed.

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. Complete the options, and click *OK*.

A group name can contain only numbers (0-9), letters (a-z, A-Z), and limited special characters (- and _).

Manage device groups

You can manage device groups from the *Device Manager* > *Device & Groups* pane. From the *Device Group* menu, select one of the following options:

Option	Description
Create New	Create a new device group.
Edit	Edit the selected device group. You cannot edit default device groups.
Delete	Delete the selected device group.

You must delete all devices from the group before you can delete the group. You must delete all device groups from an ADOM before you can delete an ADOM.

Firmware

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

View firmware for device groups

You can view firmware information for devices in a group.

To view firmware:

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

For a description of the options, see Firmware Management on page 134.

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 FortiGates*.
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.

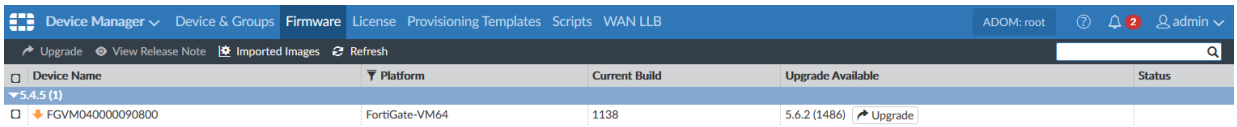
   The upgrade history is also shown, and can be viewed in more detail by selecting the *All History* icon.

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

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



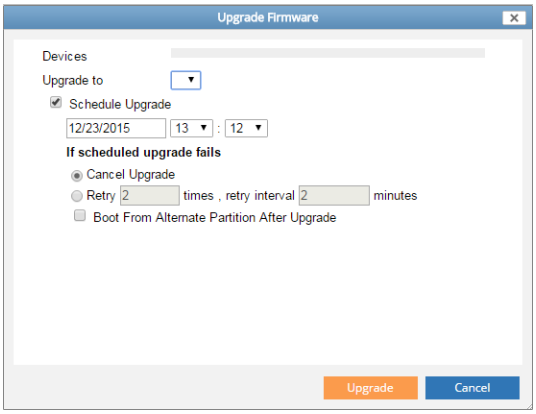
The following information and options are available:

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.
Customized Images	Select to display the customized images page, where you can import or delete images.
Refresh	Refresh the list.
Device Name	The names of the FortiGate devices in the group, organized by firmware version.
Platform	The device platform.

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 *Upgrade Firmware* dialog box.
Status	The status of the device's license. If the license has expired, the firmware cannot be upgraded.
Upgrade History	Select the icon to view the device's upgrade history in a dialog box.

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.



4. Configure the following settings:

Upgrade to	Select a firmware version from the drop-down list.
Schedule Upgrade	Select to schedule the upgrade, then enter the date and time for the upgrade, and select an action to take if the update fails: • Cancel Upgrade • Retry: enter the number of times to retry and the time between retries.
Boot From Alternate Partition After Upgrade	Select this option will cause the device to reboot twice during the upgrade process: first to upgrade the inactive partition, and second to boot back into the active partition.

5. Click *Upgrade* to update the device.

License

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

View licenses for device groups

You can view license information for devices in a group.

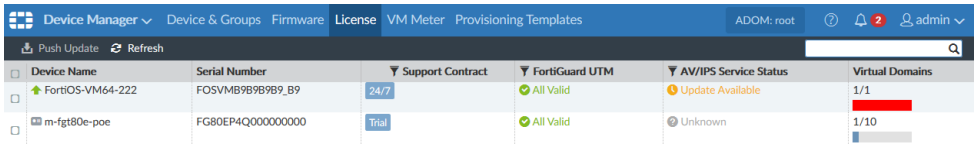
To view licenses:

1. Go to *Device Manager*.
2. In the tree menu, select a device group, and then click the *License* tab.
   For a description of the options, see License Management on page 136.

License Management

FortiGate device licenses can be updated from the *Device Manager* > *License* pane.

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



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
Support Contract	License status of the support contract. Hover over the license status to display expiration details about the following support contracts: hardware, firmware, enhanced support, and comprehensive support. License statuses: • X: 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 UTM	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 statuses: • All valid • Expires in <time> • Expired • Unknown

AV/IPS Service Status	License status of antivirus and IPS service: • Update Available • Up to Date • Expired • Unknown
Virtual Domain	Number of virtual domains. Click the cart icon to go to the Fortinet support site (https://support.fortinet.com)

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.

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 334.

Provisioning Templates

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

- System templates
- Threat Weight templates
- Certificate templates

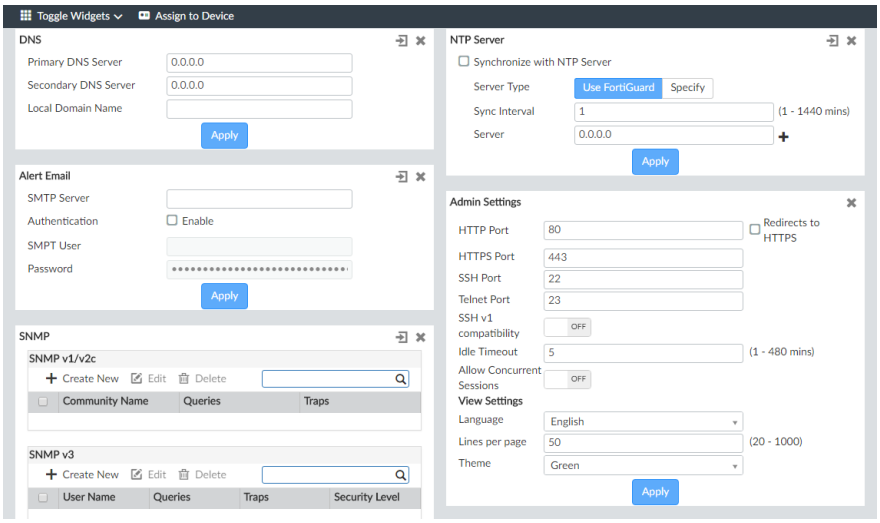
System templates

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 will be able to be linked with a system template. When linked, the selected settings will come from the template, 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.

System templates are available in 5.0, 5.2, and 5.4 ADOMs. Some settings may not be available in all ADOM versions.



The following widgets and settings are available:

Widget	Description
DNS	Primary DNS Server, Secondary DNS Server, Local Domain Name. Configure in the system template or import settings from a specific device. Select *Apply* to save the setting. Hover over the widget heading to select the following options: • Import: Import DNS settings from a specific device. Select the device in the drop-down list. Select *OK* to import settings. Select *Apply* to save the settings. • Close: Close the widget and remove it from the system template.
NTP Server	Synchronize with NTP Server and Sync Interval settings. You can select to use the FortiGuard server or specify a custom server. Configure in the system template or import settings from a specific device. Select *Apply* to save the setting. Hover over the widget heading to select the following options: • Import: Import time settings from a specific device. Select the device in the drop-down list. Select *OK* to import settings. Select *Apply* to save the settings. • Close: Close the widget and remove it from the system template.
Alert Email	SMTP Server settings including server, authentication, SMTP user, and password. Configure in the system template or import settings from a specific device. Select *Apply* to save the setting. Hover over the widget heading to select the following options: • Import: Import alert email settings from a specific device. Select the device in the drop-down list. Select *OK* to import settings. Select *Apply* to save the settings. • Close: Close the widget and remove it from the system template.
Admin Settings	Web Administration Ports, Timeout Settings, and Web Administration. Configure in the system template and select *Apply* to save the setting. Hover over the widget heading to select the following options: • Close: Close the widget and remove it from the system template.
SNMP	SNMP v1/v2 and SNMP v3 settings. In the toolbar, you can select to create, edit, or delete the record. Configure in the system template or import settings from a specific device. Select *Apply* to save the setting. Hover over the widget heading to select the following options: • Import: Import SNMP settings from a specific device. Select to import either SNMP v1/v2c or SNMP v3. Select the device in the drop-down list and the objects. Select *OK* to import settings. Select *Apply* to save the settings. • Close: Close the widget and remove it from the system template.

Widget	Description
Replacement Messages	You can customize replacement messages. Configure in the system template or import settings from a specific device. Select the import button to import settings, select the device from the drop-down list, select objects, and select *OK* to save the setting. • Hover over the widget heading to select the following options: • Close: Close the widget and remove it from the system template.
Log Settings	Send Logs to FortiAnalyzer/FortiManager (This FortiManager, Specify IP, Managed FortiAnalyzer) and Syslog settings. Configure in the system template and select *Apply* to save the settings. • Hover over the widget heading to select the following options: • Close: Close the widget and remove it from the system template.
FortiGuard	Enable FortiGuard Security Updates. Select to retrieve updates from FortiGuard servers or from this FortiManager. Select to include multiple default servers. The following options are available: • Add: Select + to add a new server. Select the server type, one of the following, *Update*, *Rating*, *Updates and Rating*. • Delete: Select an entry in the table and select - to delete the entry. • Edit: Select an entry in the table and edit the entry. Configure in the system template and select *Apply* to save the settings. • Hover over the widget heading to select the following options: • Close: Close the widget and remove it from the system template.

You can create, edit, or delete profiles. 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 that will be associated with the profile by selecting *Assign to Device*.

You can link a device to the device profile by using the *Configuration and Installation Status Wizard* from the device's system dashboard page in the *Device Manager* pane.

To assign a system template to a device:

1. Go to *Device Manager* > *Provisioning Templates* > *System Templates*.
2. In the content pane, right-click in the template row, and select *Assign to Device*.
3. Add or remove devices as needed in the *Assign to Device* dialog box, and click *OK*.

   Select the add icon to add multiple devices.

   The devices assigned to the template are shown in the *Assign To Device* column on the *System Template* content pane.

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 otherwise worth tracking.

Threat weight profiles can be created, edited, and assigned to devices. When creating a profile, the default threat level definitions are used; these can be changed later. When Threat Weight Tracking is enabled, the *Log Allowed Traffic* setting will be enabled on all policies. For more information on configuring the Threat Weight profile, see the *FortiOS Handbook*.

In FortiOS 5.2, *Client Reputation* has been renamed *Threat Weight Tracking*. In FortiOS, this feature is found at *Security Profiles* > *Advanced* > *Threat Weight*.

To create a new threat weight profile:

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

To edit a threat weight profile:

1. Right-click in the profile row, and select *Edit*. The *Edit Threat Weight*pane opens.
2. Adjust the threat levels as needed:

Log Threat Weight	Turn on threat weight tracking.
Reset	Reset all the threat level definition values back 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.

3. Click *OK* to save your changes.

To assign a threat weight profile to a device:

1. Right-click in the profile row, and select *Assign to Device*.
2. Add or remove devices as needed in the *Assign to Device* dialog box, and click *OK*. Select the add icon to add multiple devices.

   The devices assigned to the profile are shown in the *Assign To Device* column on the *Threat weight* content pane.

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 to the FortiGate device.
- The CA certificate with public key is installed to the FortiGate device.

Certificate templates are available in 5.0, 5.2, 5.4 and later ADOMs. Some settings may not be available in all ADOM versions.

The following options are available:

Create New	Create a new certificate template.
Edit	Edit a certificate template. Right-click a certificate template, and select *Edit*.
Delete	Delete a certificate template. Right-click a certificate template, and select *Delete*.
Generate	Create a new certificate from a device.

To create a new certificate template:

1. Go to *Device Manager* > *Provisioning Templates* > *Certificate Templates* .
2. Click *Create New*. The *Create New Certificate Template* pane opens.

3. Enter the following information:

Type	Specify whether the certificate uses an external or local certificate authority (CA) by selecting *Use External CA* or *Use Local CA*. When you select *Use External CA*, you must specify details about online SCEP enrollment. When you select *Use Local CA*, 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 drop-down list. The available key sizes are: • 512 Bit • 1024 Bit • 1536 Bit • 2048 Bit
Online SCEP Enrollment	
CA Server URL	Type the server URL for the external CA.
Challenge Password	Type the challenge password for the external CA server.

4. Click *OK* to create the certificate template.

To edit a certificate template:

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

To delete a certificate template:

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

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.

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.

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.

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 script options are visible in the GUI.

To enable scripts:

1. Go to *System Settings* > *Admin* > *Admin Settings*.
2. In the *Display Options on GUI* section, select the *Show Scripts* check box. For more information, see Global administrator settings on page 87.
3. Select *Apply* to apply your changes.

Configuring scripts

To configure, import, export, or run scripts, go to *Device Manager* > *Scripts*. The script list for your current ADOM will be displayed.

The following information is displayed:

Name	The user-defined script name.
Type	The script type, either *CLI* or *Tcl*.

Target	The script target. One of the following: • *Device Database* • *Policy Package, ADOM Database* • *Remote FortiGate Directly (via CLI)*
Comments	User defined comment for the script.
Last Modified	The date and time that the script was last modified.

The following options are available. Some options are available in the toolbar, and some options are available when you right-click a script.

Create New	Select to create a new script.
Import	Select to import a script from your management computer. Type a name, description, select Tcl type if applicable, and browse for the file on your management computer. Select submit to import the script to FortiManager.
Run	Select a script in the table, right-click, and select *Run* in the menu to run the script against the target selected. When selecting to run a script against a policy package, select the policy package from the drop-down list in the dialog window. When selecting to run a script against a device or database, select the device in the tree menu in the dialog window.
New	Select a script in the table, right-click, and select *New* in the menu to create a new script.
Edit	Select a script in the table, right-click, and select *Edit* in the menu to clone the script selected.
Clone	Select a script in the table, right-click, and select *Clone* in the menu to clone the script selected.
Delete	Select a script in the table, right-click, and select *Delete* in the menu to delete the script selected.
Export	Select a script in the table, right-click, and select *Export* in the menu to export the script as a `.txt` file to your management computer.
Select All	Select *Select All* in the right-click menu to select all scripts in the table and select *Delete* to delete all selected scripts.
Search	Search the scripts by typing a search term in the search field.

Run a script

You can select to enable automatic script execution or create a recurring schedule for the script.

To run a script:

1. Go to *Device Manager* > *Scripts*.
2. Select the script, then right-click and select *Run* from the menu.

Scripts can also be re-run from the script execution history by selecting the run button. See Script history on page 152 for information.

The *Execute 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 (left image below), or a policy package (right image).

3. Select a device group or devices.
4. Select *OK* to run the script.

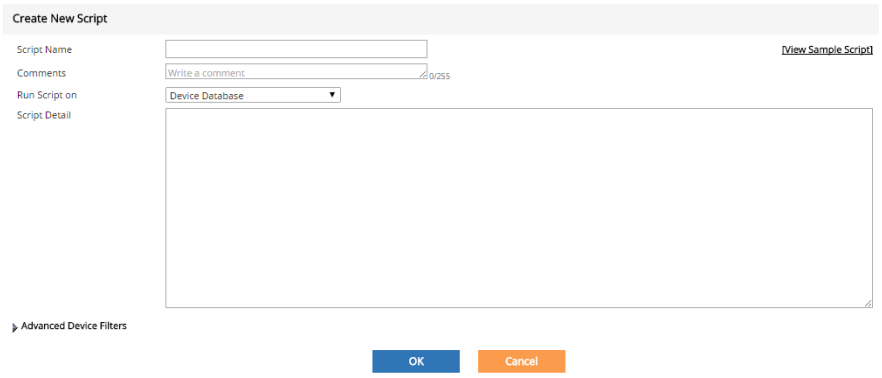
   The *Run Script* dialog box will open, showing the progress of the operation and providing information on its success or failure.

Script can also be run directly on a device using the right-click menu in *Device Manager* > *Device & Groups*.

Add a script

To add a script to an ADOM:

1. Go to *Device Manager* > *Scripts*.
2. Select *Create New*, or right-click anywhere in the script list and select *New* from the menu, to open the *Create Script* dialog box.



3. Enter the required information to create your new script.

Script Name	Type a unique name for the script.
View Sample Script	This option points to the FortiManager online help. Browse to the *Advanced Features* chapter to view sample scripts.
Comments	Optionally, type a comment for the script.

Run Script on	Select the script target. This settings will affect the options presented when you go to run a script. The options include: • *Device Database* • *Policy Package, ADOM Database* • *Remote FortiGate Directly (via CLI)*
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: • *OS Type* (select from the drop-down list) • *OS Version* (select from the drop-down list) • *Platform* (select from the drop-down list) • *Build* • *Device* (select from the drop-down list) • *Hostname* • *Serial No.*

4. Select *OK* to create the new script.

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*.
2. Right-click a script, and select *Clone*.
   The *Clone Script* pane opens, showing the exact same information as the original, except *copy_* is appended to the script name.
3. Edit the script and its settings as needed and select *OK* to create the clone.

Delete a script

To delete a script or scripts from the script list, select a script, or select multiple scripts by holding down the control or Shift keys, right-click anywhere in the script list window, and select *Delete* from the menu. Select *OK* in the confirmation dialog box to complete the deletion or, if select *Cancel* to cancel the delete.

Export a script

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

To export a script:

1. Go to *Device Manager* > *Scripts*.
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 select *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* from the toolbar. The *Import Script* dialog box opens.
3. Type a name for the script you are importing.
4. Optionally, type add a comment about the script.
5. Select the script target from the drop-down list.
6. Select *Choose File* and locate the file to be imported on your local computer.
7. Select to add advanced device filters if required.
8. Select *OK* 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 cancelled.

CLI script group

To create CLI script groups:

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:

Script Name	Enter a name for the script group.
Comments	Optionally, type a comment for the script group.
Type	CLI Script. This field is read-only.
Run Script on	Select the script target. This settings will affect the options presented when you go to run a script. The options include: • *Device Database* • *Policy Package, ADOM Database* • *Remote FortiGate Directly (via CLI)*
Available Scripts/Member Scripts	Use the directional arrows to move an available script to member scripts.

4. Select *OK* to save the CLI script group.

Script syntax

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

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

Syntax applicable for address and address6

```
config firewall address
   edit xxxx

      ...regular FOS command here...

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

Syntax applicable for ippool and ippool6

```
config firewall ippool
   edit xxxx

      ...regular FOS command here...

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

Syntax applicable for vip, vip6, vip46, and vip64

```
config firewall vip
   edit xxxx

      ...regular FOS command here...

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

Syntax applicable for dynamic zone

```
config dynamic interface
   edit xxxx
      set single-intf disable
      set default-mapping enable|disable
```

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

Syntax applicable for dynamic interface

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

Syntax applicable for dynamic multicast interface

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

Syntax applicable for local certificate (dynamic mapping)

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

Syntax applicable for vpn tunnel

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

```
    end
```

Syntax applicable for vpn console table

```
config vpnmgr vpntable
   edit xxxx
      set topology star|meshed|dial
      set psk-auto-generate enable|disable
      set psksecret xxxx
      set ike1proposal 3des-sha1 3des-md5 ...
      set ike1dhgroup XXXX
      set ike1keylifesec 28800
      set ike1mode aggressive|main
      set ike1dpd enable|disable
      set ike1nattraversal enable|disable
      set ike1natkeepalive 10
      set ike2proposal 3des-sha1 3des-md5
      set ike2dhgroup 5
      set ike2keylifetype seconds|kbyte|both
      set ike2keylifesec 1800
      set ike2keylifekbs 5120
      set ike2keepalive enable|disable
      set replay enable|disable
      set pfs enable|disable
      set ike2autonego enable|disable
      set fcc-enforcement enable|disable
      set localid-type auto|fqdn|user-fqdn|keyid|addressasn1dn
      set authmethod psk|signature
      set inter-vdom enable|disable
      set certificate XXXX
   next
end
```

Syntax applicable for vpn console node

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

```
        next
    end
```

Syntax applicable for setting installation target on policy package

```
config firewall policy
   edit x

      ...regular policy command here...

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

Syntax applicable for global policy

```
config global header policy

   ...regular policy command here...

end

config global footer policy

   ...regular policy command here...

end
```

Script history

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

To view the script execution history:

1. In *Device Manager*, locate the device whose script history you want to view.
2. In the content pane, select *Dashboard*, and find the *Configuration and Installation Status* widget.
3. Select *View History* in the *Script Status* field to open the *Script Execution History* pane.
4. 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.
5. 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 145.
6. 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 353.

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 158.

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 158.

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 telnet 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

```
show route static
```

Output

```
config router static
   edit 1
      set device "port1"
      set gateway 172.20.120.2
   next
   edit 2
      set device "port2"
      set distance 7
      set dst 172.20.120.0 255.255.255.0
      set gateway 172.20.120.2
   next
end
```

Variations none

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

Script

```
config global
   diag debug rating
end
```

Output

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

```
------- Executing time: 2013-10-15 14:32:15 ------
Starting log (Run on device)
FortiGate-VM64 $ config global
FortiGate-VM64 (global) $ diagnose debug rating
Locale : english
License : Contract
Expiration : Thu Jan 3 17:00:00 2030
-=- Server List (Tue Oct 15 14:32:49 2013) -=-
IP Weight RTT Flags TZ Packets Curr Lost Total Lost
192.168.100.206 35 2 DIF -8 4068 72 305
192.168.100.188 36 2 F -8 4052 72 308
FortiGate-VM64 (global) $ end
------- The end of log ----------
```

Variations

Output for this script will vary based on the state of the FortiGate device. The preceding output is for a FortiGate device that has never been registered.
For a registered FortiGate device without a valid license, the output would be similar to:

```
Locale : english
License : Unknown
Expiration : N/A
Hostname : guard.fortinet.net

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

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

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

```
config global
   config system accprofile
      edit "policy_admin"
         set fwgrp read
         set loggrp read
         set sysgrp read
      next
   end
end
```

Output	View the log of script running on device:FortiGate-VM64
	`------- Executing time: 2013-10-16 13:39:35 ------`
	`Starting log (Run on device)`
	`FortiGate-VM64 $ config global`
	`FortiGate-VM64 (global) $ config system accprofile`
	`FortiGate-VM64 (accprofile) $ edit "prof_admin"`
	`FortiGate-VM64 (prof_admin) $ set fwgrp read`
	`FortiGate-VM64 (prof_admin) $ set loggrp read`
	`FortiGate-VM64 (prof_admin) $ set sysgrp read`
	`FortiGate-VM64 (prof_admin) $ next`
	`FortiGate-VM64 (accprofile) $ end`
	`FortiGate-VM64 (global) $ end`
	`------- The end of log ----------`

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

With the introduction of global objects/security console (global database), you can run a CLI script on the FortiManager global database in addition to running it on a FortiGate unit directly. Compare the following sample scripts:

- Running a CLI script on a FortiGate unit

```
config vdom
   edit "root"
      config firewall policy
         edit 10
            set srcintf "port5"
            set dstintf "port6"
            set srcaddr "all"
            set dstaddr "all"
            set status disable
            set schedule "always"
            set service "ALL"
            set logtraffic disable
      next
end
```

- Running a CLI script on the global database

```
config firewall policy
   edit 10
      set srcintf "port5"
      set dstintf "port6"
      set srcaddr "all"
      set dstaddr "all"
      set status disable
      set schedule "always"
      set service "ALL"
      set logtraffic disable
   next
end
```

Error Messages

Most error messages you will see are regular FortiGate CLI error messages. If you are familiar with the CLI you will likely recognize them.

Other error messages indicate your script encountered problems while executing, such as:

- `command parse error`: It was not possible to parse this line of your script into a valid FortiGate CLI command. Common causes for this are misspelled keywords or an incorrect command format.
- `unknown action`: Generally this message indicates the previous line of the script was not executed, especially if the previous line accesses an object such as “config router static”.
- `Device XXX failed-1`: This usually means there is a problem with the end of the script. XXX is the name of the FortiGate unit the script is to be executed on. If a script has no end statement or that line has an error in it you may see this error message. You may also see this message if the FortiGate unit has not been synchronized by deploying its current configuration.

Troubleshooting Tips

Here are some troubleshooting tips to help locate and fix problems you may experience with your scripts.

- Check the script output. Generally the error messages displayed here will help you locate and fix the problem.
- See the *FortiGate CLI Reference* for more information on all CLI commands.
- There is a limit to the number of scripts allowed on the FortiManager unit. Try removing an old script before trying to save your current one.
- As mentioned at the start of this chapter, ensure the `console more` command is disabled on the FortiGate devices where scripts execute. Otherwise a condition may occur where both the FortiGate device and the FortiManager system are waiting for each other to respond until they timeout.
- There should be no punctuation at the start or end of the lines.
- Only whitespace is allowed on the same line as the command. This is useful in lining up `end` and `next` commands for quick and easy debugging of the script.
- Keep your scripts short. They are easier to troubleshoot and it gives you more flexibility. You can easily execute a number of scripts after each other.
- Use full command names. For example instead of “set host test” use “set hostname test”. This is required for any scripts that are to be run on the global database.
- Use the number sign (#) to comment out a line you suspect contains an error.

Tcl scripts

Tcl is a dynamic scripting language that extends the functionality of CLI scripting. In FortiManager Tcl scripts, the first line of the script is “#!” as it is for standard Tcl scripts.

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 http://www.tcl.tk.

Tcl scripts can do more than just get and set information. The benefits of Tcl come from:

- variables to store information,
- loops to repeats commands that are slightly different each time
- decisions to compare information from the device

The sample scripts in this section will contain procedures that you can combine to use your scripts. The samples will each focus on one of four areas:

- Tcl variables
- Tcl loops
- Tcl decisions
- Tcl file IO

To enable Tcl scripting, use the following CLI commands:

```
config system admin setting
   set show_tcl_script enable
end
```

Limitations of FortiManager Tcl

FortiManager Tcl executes in a controlled environment. You do not have to know the location of the Tcl interpreter or environment variables to execute your scripts. This also means some of the commands normally found in Tcl are not used in FortiManager Tcl.

Depending on the CLI commands you use in your Tcl scripts, you may not be able to run some scripts on some versions of FortiOS as CLI commands change periodically.

Before testing a new script on a FortiGate device, you should backup that device's configuration and data to ensure it is not lost if the script does not work as expected.

Tcl variables

Variables allow you to store information from the FortiGate device, and use it later in the script. Arrays allow you to easily manage information by storing multiple pieces of data under a variable name. The next script uses an array to store the FortiGate system information.

Example: Save system status information in an array.

Script:

```
#!
proc get_sys_status aname {
   upvar $aname a
puts [exec "# This is an example Tcl script to get the system status of the FortiGate\n"
    "# " 15 ]
   set input [exec "get system status\n" "# " 15 ]
# puts $input
   set linelist [split $input \n]
# puts $linelist
foreach line $linelist {
   if {![regexp {([^:]+):(.*)} $line dummy key value]} continue
      switch -regexp -- $key {
      Version {
```

```
      regexp {FortiGate-([^ ]+) ([^,]+),build([\d]+),.*} $value dummy a(platform) a
          (version) a(build)
   }
Serial-Number {
   set a(serial-number) [string trim $value]
}
   Hostname {
      set a(hostname) [string trim $value]
      } }
   }
}
get_sys_status status
puts "This machine is a $status(platform) platform."
puts "It is running version $status(version) of FortiOS."
puts "The firmware is build# $status(build)."
puts "S/N: $status(serial-number)"
puts "This machine is called $status(hostname)"
```

Output:

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

FortiGate-VM64 #

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

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

Variations:

Once the information is in the variable array, you can use it as part of commands you send to the FortiGate device or to make decisions based on the information. For example:

```
if {$status(version) == 5.0} {
# follow the version 5.0 commands
} elseif {$status(version) == 5.0} {
# follow the version 5.0 commands
}
```

This script introduces the concept of executing CLI commands within Tcl scripts using the following method:

```
set input [exec "get system status\n" "# "]
```

This command executes the CLI command "`get system status`" and passes the result into the variable called `input`. Without the "\n" at the end of the CLI command, the CLI command will not execute to provide output.

In analyzing this script:

- line 1 is the required #! to indicate this is a Tcl script
- lines 2-3 open the procedure declaration
- lines 4-5 puts the output from the CLI command into a Tcl variable as a string, and breaks it up at each return character into an array of smaller strings
- line 6 starts a loop to go through the array of strings
- line 7 loops if the array element is punctuation or continues if its text

- line 8 takes the output of line 7's regular expression command and based on a match, performs one of the actions listed in lines 9 through 17
- lines 9-11 if regular expression matches 'Version' then parse the text and store values for the platform, version, and build number in the named array elements
- line 12-14 if regular expression matches 'Serial-Number' then store the value in an array element named that after trimming the string down to text only
- lines 15-17 is similar to line 12 except the regular expression is matched against 'Hostname'
- line 17-19 close the switch decision statement, the for each loop, and the procedure
- line 20 calls the procedure with an array name of status
- lines 21-25 output the information stored in the status array

Tcl loops

Even though the last script used a loop, that script's main purpose was storing information in the array. The next script uses a loop to create a preset number of users on the FortiGate device, in this case 10 users. The output is only shown for the first two users due to space considerations.

Example: Create 10 users from usr0001 to usr0010:

Script:

```
#!
proc do_cmd {cmd} {
puts [exec "$cmd\n" "# " 15]
}
   set num_users 10
do_cmd "config vdom"
do_cmd "edit root"
do_cmd "config user local"
for {set i 1} {$i <= $num_users} {incr i} {
   set name [format "usr%04d" $i]
   puts "Adding user: $name"
   do_cmd "edit $name"
   do_cmd "set status enable"
   do_cmd "set type password"
   do_cmd "next"
}
do_cmd "end"
do_cmd "end"

do_cmd "config vdom"
do_cmd "edit root"
do_cmd "show user local"
do_cmd "end"
```

Output:

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

------- Executing time: 2013-10-16 15:27:18 ------
Starting log (Run on device)
config vdom
FortiGate-VM64 (vdom) #
edit root
current vf=root:0
FortiGate-VM64 (root) #
```

```
config user local
FortiGate-VM64 (local) #
Adding user: usr0001
edit usr0001
new entry 'usr0001' added
FortiGate-VM64 (usr0001) #
set status enable
FortiGate-VM64 (usr0001) #
set type password
FortiGate-VM64 (usr0001) #
next

FortiGate-VM64 (local) #
Adding user: usr0002
edit usr0002
new entry 'usr0002' added
FortiGate-VM64 (usr0002) #
set status enable
FortiGate-VM64 (usr0002) #
set type password
FortiGate-VM64 (usr0002) #
next
```

Variations:

There are a number of uses for this kind of looping script. One example is to create firewall policies for each interface that deny all non-HTTPS and non-SSH traffic by default. Another example is a scheduled script to loop through the static routing table to check that each entry is still reachable, and if not remove it from the table.

This script loops 10 times creating a new user each time whose name is based on the loop counter. The format command is used to force a four digit number.

In analyzing this script:

- line 1 is the required #! to indicate this is a Tcl script
- lines 2-4 open CLI command wrapper procedure
- line 5 declares the number of users to create
- line 6 gets the FortiGate ready for entering local users
- line 7 opens the for loop that will loop ten times
- line 8 sets the user name based on the incremented loop counter variable
- line 9 is just a comment to the administrator which user is being created
- lines 10-13 create and configure the user, leaving the CLI ready for the next user to be added
- line 14 ends the for loop
- line 15 ends the adding of users in the CLI
- line 16 executes a CLI command to prove the users were added properly

Tcl decisions

Tcl has a number of decision structures that allow you to execute different CLI commands based on what information you discover.

This script is more complex than the previous scripts as it uses two procedures that read FortiGate information, make a decision based on that information, and then executes one of the CLI sub-scripts based on that information.

Example: Add information to existing firewall policies.

Script:

```
#!
# need to define procedure do_cmd
# the second parameter of exec should be "# "
# If split one command to multiple lines use "\" to continue
proc do_cmd {cmd} {
   puts [exec "$cmd\n" "# "]
}
foreach line [split [exec "show firewall policy\n" "# "] \n] {
   if {[regexp {edit[ ]+([0-9]+)} $line match policyid]} {
      continue
   } elseif {[regexp {set[ ]+(\w+)[ ]+(.*)\r} $line match key value]} {
      lappend fw_policy($policyid) "$key $value"
   }
}
do_cmd "config firewall policy"
foreach policyid [array names fw_policy] {
   if {[lsearch $fw_policy($policyid){diffservcode_forward 000011}] == -1} {
      do_cmd "edit $policyid"
      do_cmd "set diffserv-forward enable"
      do_cmd "set diffservcode-forward 000011"
      do_cmd "next"
   }
}
do_cmd "end"
```

Variations:

This type of script is useful for updating long lists of records. For example if the FortiOS version adds new keywords to user accounts, you can create a script similar to this one to get the list of user accounts and for each one edit it, add the new information, and move on to the next.

This script uses two decision statements. Both are involved in text matching. The first decision is checking each line of input for the policy ID and if its not there it skips the line. If it is there, all the policy information is saved to an array for future use. The second decision searches the array of policy information to see which polices are miss

In analyzing this script:

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

Additional Tcl Scripts

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

Script:

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

Output:

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

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

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

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

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

Example: Configure common global settings.

Script:

```
#!
#Run on FortiOS v5.00
#This script will configure common global, user group and ntp settings
#if you do not want to set a parameter, comment the
```

```
#corresponding set command
#if you want to reset a parameter to it's default
#value, set it an empty string
puts [exec "# This is an example Tcl script to configure global, user group and ntp
    setting of FortiGate\n" "# " 15 ]

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

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

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

```
fgt_cmd "end"
fgt_cmd "end"
#config system ntp---end
```

Output:

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

FortiGate-VM64 # config global
FortiGate-VM64 (global) # config system global
FortiGate-VM64 (global) # unset admintimeout
FortiGate-VM64 (global) # end
FortiGate-VM64 (global) # end
FortiGate-VM64 # config vdom
FortiGate-VM64 (vdom) # edit root
current vf=root:0
FortiGate-VM64 (root) # config user group
FortiGate-VM64 (group) # edit groupname
FortiGate-VM64 (groupname) # set authtimeout 20
FortiGate-VM64 (groupname) # end
FortiGate-VM64 (root) # end
FortiGate-VM64 # config global
FortiGate-VM64 (global) # config system ntp
FortiGate-VM64 (ntp) # set ntpsync enable
FortiGate-VM64 (ntp) # set source-ip 0.0.0.0
FortiGate-VM64 (ntp) # end
FortiGate-VM64 (global) # end
FortiGate-VM64 #
------- The end of log ----------
```

Example: Configure syslogd settings and filters.

Script:

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

```
   set len [llength $kv]
if {$len == 0} {
continue
} elseif {$len == 1} {
fgt_cmd "unset [lindex $kv 0]"
} else {
fgt_cmd "set [lindex $kv 0] [lindex $kv 1]"
} } }
#configure log syslogd setting---begin
fgt_cmd "config global"
fgt_cmd "config log syslogd$syslogd_no setting"
   set_kv $setting_list
fgt_cmd "end"
#configure log syslogd setting---end
#configure log syslogd filter---begin
fgt_cmd "config log syslogd$syslogd_no filter"
   set_kv $filter_list
fgt_cmd "end"
#configure log syslogd filter---end
```

Output:

```
Starting log (Run on device)

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

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

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

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

Script:

```
#!
#This script will configure the FortiGate device to
#communicate with a FortiAnalyzer unit
#Enter the following key-value pairs for 'config
#system fortianalyzer'
   set status enable
   set enc-algorithm high
#localid will be set as the hostname automatically
#later
```

```
puts [exec "# This is an example Tcl script to configure the FortiGate to communicate with
    a FortiAnalyzer\n" "# " 15 ]
   set server 1.1.1.1
#for fortianalyzer, fortianalyzer2 or
#fortianalyzer3, enter the corresponding value "",
#"2", "3"
   set faz_no ""
#keys used for 'config system fortianalyzer', if you
#do not want to change the value of a key, do not put
#it in the list
   set key_list {status enc-algorithm localid server }
##procedure to get system status from a FortiGate
proc get_sys_status aname {
upvar $aname a
set input [split [exec "get system status\n" "# "] \n]
foreach line $input {
if {![regexp {([^:]+):(.*)} $line dummy key value]} continue
   set a([string trim $key]) [string trim $value]
}
}
#procedure to execute FortiGate command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# "]
}
#set the localid as the FortiGate's hostname
get_sys_status sys_status
set localid $sys_status(Hostname)
#config system fortianalyzer---begin
fgt_cmd "config global"
fgt_cmd "config log fortianalyzer$faz_no setting"
foreach key $key_list {
if [info exists $key] {
   fgt_cmd "set $key [set $key]"
} else {
   fgt_cmd "unset $key"
}
}
fgt_cmd "end"
fgt_cmd "end"
#config system fortianalyzer---end
```

Output:

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

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

Script:

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

puts [exec "# This is an example Tcl script to create custom ips signatures and change the
    settings for the custom ips signatures on a FortiGate\n" "# " 15 ]
#Enter custom ips signatures, signature names are the
#names of array elements
   set custom_sig(c1) {"F-SBID(--protocol icmp;--icmp_type 10; )"}
   set custom_sig(c2) {"F-SBID(--protocol icmp;--icmp_type 0; )"}
#Enter custom ips settings
   set custom_rule(c1) {{status enable} {action block} {log enable} {log-packet} {severity
       high}}
   set custom_rule(c2) {{status enable} {action pass} {log} {log-packet disable} {severity
       low}}
#procedure to execute FortiGate command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# "]
}
#procedure to set a series of key-value pairs
proc set_kv kv_list {
foreach kv $kv_list {
set len [llength $kv]
if {$len == 0} {
   continue
} elseif {$len == 1} {
   fgt_cmd "unset [lindex $kv 0]"
} else {
   fgt_cmd "set [lindex $kv 0] [lindex $kv 1]"
}
} }
#config ips custom---begin
fgt_cmd "config vdom"
fgt_cmd "edit root"
fgt_cmd "config ips custom"
foreach sig_name [array names custom_sig] {
fgt_cmd "edit $sig_name"
fgt_cmd "set signature $custom_sig($sig_name)"
fgt_cmd "next"
}
fgt_cmd "end"
#config ips custom settings---begin
foreach rule_name [array names custom_rule] {
fgt_cmd "config ips custom"
fgt_cmd "edit $rule_name"
set_kv $custom_rule($rule_name)
fgt_cmd "end"
}
fgt_cmd "end"
#config ips custom settings---end
```

Output:

```
Starting log (Run on device)
FortiGate-VM64 # config vdom
FortiGate-VM64 (vdom) # edit root
current vf=root:0
FortiGate-VM64 (root) # config ips custom
```

```
FortiGate-VM64 (custom) # edit c1
set signature "F-SBID(--protocol icmp;--icmp_type 10; )"
FortiGate-VM64 (c1) # set signature "F-SBID(--protocol icmp;--icmp_type 10; )"
FortiGate-VM64 (c1) # next
FortiGate-VM64 (custom) # edit c2
FortiGate-VM64 (c2) # set signature "F-SBID(--protocol icmp;--icmp_type 0; )"
FortiGate-VM64 (c2) # next
FortiGate-VM64 (custom) # end
FortiGate-VM64 (root) # config ips custom
FortiGate-VM64 (custom) # edit c1
FortiGate-VM64 (c1) # set status enable
FortiGate-VM64 (c1) # set action block
FortiGate-VM64 (c1) # set log enable
FortiGate-VM64 (c1) # unset log-packet
FortiGate-VM64 (c1) # set severity high
FortiGate-VM64 (c1) # end
FortiGate-VM64 (root) # config ips custom
FortiGate-VM64 (custom) # edit c2
FortiGate-VM64 (c2) # set status enable
FortiGate-VM64 (c2) # set action pass
FortiGate-VM64 (c2) # unset log
FortiGate-VM64 (c2) # set log-packet disable
FortiGate-VM64 (c2) # set severity low
FortiGate-VM64 (c2) # end
FortiGate-VM64 (root) # end
FortiGate-VM64 #
------- The end of log ----------
```

Variations:

None.

Tcl file IO

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

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

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

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

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

To write to a file:

Script

```
#!
set somefile [open “tcl_test” w]
puts $somefile "Hello, world!"
close $somefile
```

To read from a file:	

Script	#!
	set otherfile [open “tcl_test” r]
	while {[gets $otherfile line] >= 0} {
	puts [string length $line]
	}
	close $otherfile

Output	Hello, world!

These two short scripts write a file called `tcl_test` and then read it back.

Line 3 in both scripts opens the file either for reading (r) or writing (w) and assigns it to a filehandle (somefile or otherfile). Later in the script when you see these filehandles, its input or output passing to the open file.

When reading from the file, lines 4 and 5 loop through the file line by line until it reaches the end of the file. Each line that is read is put to the screen.

Both scripts close the file before they exit.

Troubleshooting Tips

This section includes suggestions to help you find and fix problems you may be having with your scripts.

- Make sure the commands you are trying to execute are valid for the version of FortiOS running on your target FortiGate device.
- 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).

Example 1:

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

Syntax

```
puts [exec_ondb "/adom/<adom_name>/pkg/<pkg_fullpath>"
    "embedded cli commands" "# "]
```

Usage

```
puts [exec_ondb "/adom/52/pkg/default" "
config firewall address
edit port5_address
next
end
" "# "]
```

Example 2:

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

Syntax

```
puts [exec_ondb "/adom/./pkg/<pkg_fullpath>" "embedded cli
    commands" "# "]
```

or

```
puts [exec_ondb "/pkg/<pkg_fullpath>" "embeded cli commands"
    "# "]
```

Usage

```
puts [exec_ondb "/adom/./pkg/default" "
config firewall address
edit port5_address
next
end
" "# "]
```

Example 3:

Run Tcl script on a specific device in an ADOM:

Syntax

```
puts [exec_ondb "/adom/<adom_name>/device/<dev_name>"
    "embedded cli commands" "# "]
```

Usage

```
puts [exec_ondb "/adom/v52/device/FGT60CA" "
config global
config system global
set admintimeout 440
end
end
" "# "]
```

Example 4:

Run Tcl script on current devices in an ADOM:

Syntax	`puts [exec_ondb "/adom/<adom_name>/device/." "embedded cli commands" "# "]`
Usage	`puts [exec_ondb "/adom/v52/device/." " config global config system global set admintimeout 440 end end " "# "]`

`exec_ondb` cannot be run on the Global ADOM.

WAN Link Load Balance

When central monitoring is enabled, you can use the *Device Manager* > *WAN LLB* > *WAN Status Check Profiles* pane to monitor load-balancing profiles of WAN links. When central monitoring is disabled, you must monitor load-balancing profiles by monitoring each device.

Enabling central monitoring of load balancing

You can enable centralized WAN link load balancing 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 central monitoring, you use the *Device Manager* > *WAN Link Load Balance* > *Status Check Profiles* pane for centrally monitoring WAN link load balancing.

To enable when ADOMs enabled:

1. Go to *System Settings* > *All ADOMs*.
2. Right-click an ADOM, and select *Edit*.
3. Beside Central Management, select the *WAN Link Load Balance* check box.
4. Click *OK*. Central monitoring of WAN link load balancing is enabled for the ADOM.

To enable when ADOMs disabled:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, beside *WAN Link Load Balance*, click *Change WAN Link Load Balance Mode*. The *Change WAN Link Load Balance Mode* dialog box is displayed.
3. Click *OK*.

Creating load balancing profiles

You can create a load balancing profile for WAN links of a device.

To create a load balancing profile:

1. Ensure that you are in the correct ADOM.
2. Go to *Device Manager* > *WAN LLB* and click *Create New*. The *New WAN LLB* pane opens.
3. Configure the following options:

Device	Select a FortiGate device with WAN links.
Name	Displays the name of the profile.
Type	Displays the type of profile.
Administrative Status	Enable or disable the profile. Select *Up* to enable the profile, or select *Down* to disable the profile.
WAN LLB	
Load Balance Algorithm	Select a load-balancing algorithm: • Volume • Sessions • Spillover • Source-Destination IP • Source IP
Interface Members	Specify the interface members for which you want to balance loads. The interface members are derived from the FortiGate device. Click *Create New* to add interfaces. Select the interface, gateway IP, and status of the interface member, then click *OK* to add the interface member. Interface members can also be edited and delete from the list.
WAN LLB Rules	Specify the priority rules for load balancing. The priority rules are derived from the FortiGate device. Click *Create New* to add a priority rule. Enter the name of the service, then select the source address and user groups, destination address and protocol number, outgoing interface, and health check, then click *OK* to add the rule. Rules can also be edited and deleted from the list.

4. Click *OK* to add the WAN link.

Manage load balancing profiles

You can manage load balancing profiles from the *Device Manager* > *WAN LLB* pane. Some options are located in the toolbar, and some options are available when you right-click a profile in the content pane.

Option	Description
Create New	Create a new load-balancing profile.
Delete	Delete the selected profile.
Edit	Edit the selected profile.
Select All	Select all profiles in the content pane.

Creating profiles for checking WAN link status

When central monitoring of WAN link load balancing is enabled, you can create profiles that monitor the status of load-balancing profiles for WAN links.

To create a profile:

1. If necessary, ensure that you are in the correct ADOM.
2. Go to *Device Manager* > *WAN LLB* > *WAN Status Check Profile*, and click *Create New*. The *New WAN Status Check Profile* pane opens.
3. Configure the following options:

Name	Enter a name for the profile.
Detect Protocol	Select the detection method for the profile check: • Ping • TCP Echo • UDP Echo • HTTP • TWAMP
Detect Server	Type the IP address for WAN interface that you want to monitor.
Link Status	Specify options for the WAN link status.
Timeout	Specify how many seconds before the link times out.
Failures before inactive	Specify the threshold that triggers a warning message, in milliseconds, or percent if the criteria is *Packet Loss*.
Restore link after	Specify the threshold that triggers an error message, in milliseconds, or percent if the criteria is *Packet Loss*.
Actions 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

4. Click *OK* to create the new status check profile.

Manage profiles for checking WAN link status

When central monitoring of WAN link load balancing is enabled, you can manage monitoring profiles from the *Device Manager* > *WAN LLB* > *WAN Status Check Profile* pane. Some options are located in the toolbar, and some options are available when you right-click a profile.

Option	Description
Create New	Create a new profile for checking WAN link status.
Delete	Delete the selected profile.
Edit	Edit the selected profile.
Clone	Clone the selected profile.
Select All	Select all profiles in the content pane.

FortiExtender

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

FortiExtender can be managed by a FortiGate running FortiOS v5.2 or later.

Centrally managed

When managing FortiExtender centrally, FortiAP devices will be listed in the *AP Management* pane in the ADOM of the FortiGate managing the FortiExtender.

The following information is displayed:

Device Name	The serial number of the FortiGate device that is managing the FortiExtender.
Serial Number	The serial number of the FortiExtender.
Priority	The FortiExtender priority, either *Primary* or *Secondary*.
Model	The FortiExtender model.
Management Status	The FortiExtender management status, either *Authorized* or *Deauthorized*.

Status	The FortiExtender status, either *Up* or *Down*.
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.

The right-click menu options include:

Refresh	Select a FortiExtender in the list, right-click, and select *Refresh* in the menu to refresh the information displayed.
Edit	Select a FortiExtender in the list, right-click, and select *Edit* in the menu to edit the FortiExtender modem settings, PPP authentication, general, GSM/LTE, and CDMA settings.
Upgrade	Select a FortiExtender in the list, right-click, and select *Upgrade* in the menu to upgrade the FortiExtender firmware.
Authorize	Select a FortiExtender in the list, right-click, and select *Authorize* in the menu to authorize the unit for management.
Deauthorize	Select a FortiExtender in the list, right-click, and select *Deauthorize* in the menu to deauthorize the unit for management.
Restart	Select a FortiExtender in the list, right-click, and select *Restart* in the menu to restart the unit.
Set Primary	Select a FortiExtender in the list, right-click, and select *Set Primary* in the menu to set the unit as the primary device.
Status	Select a FortiExtender in the list, right-click, and select *Status* in the menu to view status information including system status, modem status, and data usage.

To edit a FortiExtender:

1. Go to *Device Manager* > *FortiExtender* .
2. Right-click the FortiExtender device, and select *Edit* . The *Edit FortiExtender* page is displayed.
3. Configure the following settings:

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 the allow 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.

4. Select *OK* to save the setting.

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 a FortiOS VM 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-v5-buildXXXX-Fortinet.out`. In FortiManager, the VM will be listed as a FortiOS VM.

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-v5xx-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/) 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 registered to the FortiManager. See Adding devices on page 95.
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

Point 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.

Authorizing metered VMs

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

Authorizing FortiOS VMs

FortiOS VMs must be registered before they can be authorized. See Adding devices on page 95.

To authorize metered FortiOS VMs:

1. Ensure that the VM is registered to the FortiManager. See Adding devices on page 95.
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 servies.
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 registered manually before they can be authorized. See Adding devices manually on page 102.

To authorize metered FortiWeb VMs:

1. Ensure that the FortiWeb VM is registered to the FortiManager. See Adding devices on page 95.
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 371 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:

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 drop-down 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.

4. Select *OK*.

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 drop-down list of a slot, select a FortiGate-5000 series blade to assign it to the slot. You can select a FortiGate, FortiCarrier, or FortiSwitch unit.

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

5. Click *OK*.

Viewing chassis dashboard

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

Viewing the status of the FortiGate blades

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

The following is displayed:

Refresh	Select to update the current page. If there are no entries, Refresh is not displayed.
Slot #	The slot number in the chassis. The FortiGate 5050 chassis contains five slots numbered 1 to 5. The FortiGate 5060 chassis contains six slots numbered 1 to 6. The FortiGate 5140 and 5140B chassis contains fourteen slots numbered 1 to 14.
Extension Card	If there is an extension card installed in the blade, this column displays an arrow you can select to expand the display. The expanded display shows details about the extension card as well as the blade.
Slot Info	Indicates whether the slot contains a node card (for example, a FortiGate 5001SX blade) or a switch card (for example, a FortiSwitch 5003 blade) or is empty.
State	Indicates whether the card in the slot is installed or running, or if the slot is empty.

Temperature Sensors	Indicates if the temperature sensors for the blade in each slot are detecting a temperature within an acceptable range. *OK* indicates that all monitored temperatures are within acceptable ranges. *Critical* indicates that a monitored temperature is too high (usually about 75°C or higher) or too low (below 10°C).
Current Sensors	Indicates if the current sensors for the blade in each slot are detecting a current within an acceptable range. *OK* indicates that all monitored currents are within acceptable ranges. *Critical* indicates that a monitored current is too high or too low.
Voltage Sensors	Indicates if the voltage sensors for the blade in each slot are detecting a voltage within an acceptable range. *OK* indicates that all monitored voltages are within acceptable ranges. *Critical* indicates that a monitored voltage is too high or too low.
Power Allocated	Indicates the amount of power allocated to each blade in the slot.
Action	Select *Activate* to turn the state of a blade from *Installed* into *Running*. Select *Deactivate* to turn the state of a blade from *Running* into *Installed*.
Edit	Select to view the detailed information on the voltage and temperature of a slot, including sensors, status, and state. You can also edit some voltage and temperature values.
Update	Select to update the slot.

To edit voltage and temperature values:

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

Viewing the status of the power entry modules

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

The following is displayed:

Refresh	Select to update the current page.
PEM	The order numbers of the PEM in the chassis.

Presence	Indicates whether the PEM is present or absent.
Temperature	The temperature of the PEM.
Temperature State	Indicates whether the temperature of the PEM is in the acceptable range. *OK* indicates that the temperature is within acceptable range.
Threshold	PEM temperature thresholds.
Feed -48V	Number of PEM fuses. There are four pairs per PEM.
Status	PEM fuse status: present or absent.
Power Feed	The power feed for each pair of fuses.
Maximum External Current	Maximum external current for each pair of fuses.
Maximum Internal Current	Maximum internal current for each pair of fuses.
Minimum Voltage	Minimum voltage for each pair of fuses.
Power Available	Available power for each pair of fuses.
Power Allocated	Power allocated to each pair of fuses.
Used By	The slot that uses the power.

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

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

The following is displayed:

Refresh	Select to update the current page.
Thresholds	Displays the fan tray thresholds.
Fan Tray	The order numbers of the fan trays in the chassis.
Model	The fan tray model.
24V Bus	Status of the 24V Bus: present or absent.
-48V Bus A	Status of the -48V Bus A: present or absent.
-48V Bus B	Status of the -48V Bus B: present or absent.
Power Allocated	Power allocated to each fan tray.

Fans	Fans in each fan tray.
Status	The fan status. *OK* means it is working normally.
Speed	The fan speed.

Viewing shelf manager status

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

The following is displayed:

Refresh	Select to update the current page.
Shelf Manager	The order numbers of the shelf managers in the chassis.
Model	The shelf manager model.
State	The operation status of the shelf manager.
Temperature	The temperature of the shelf manager.
-48V Bus A	Status of the -48V Bus A: present or absent.
-48V Bus B	Status of the -48V Bus B: present or absent.
Power Allocated	Power allocated to each shelf manager.
Voltage Sensors	Lists the voltage sensors for the shelf manager.
State	Indicates if the voltage sensors for the shelf manager are detecting a voltage within an acceptable range. *OK* indicates that all monitored voltages are within acceptable ranges. *Below lower critical* indicates that a monitored voltage is too low.
Voltage	Voltage value for a voltage sensor.
Edit	Select to modify the thresholds of a voltage sensor.

Viewing shelf alarm panel (SAP) status

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

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

The following is displayed:

Presence	Indicates if the SAP is present or absent.

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

Policy & Objects

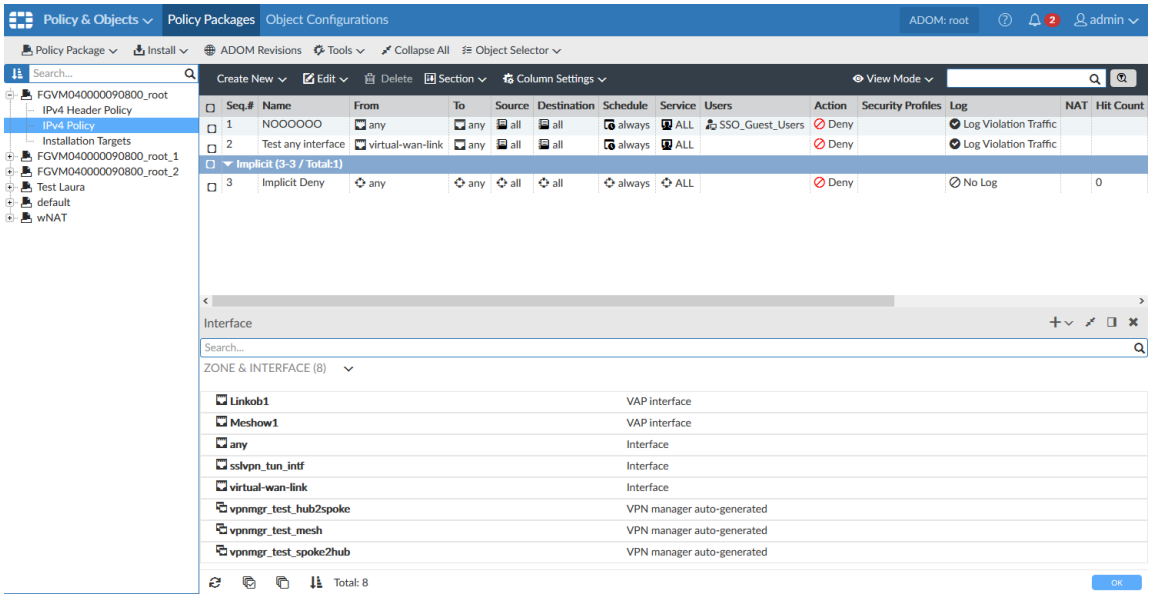
The *Policy & Objects* pane enables you to centrally manage and configure the devices that are managed by the FortiManager unit. This includes the basic network settings to connect the device to the corporate network, antivirus definitions, intrusion protection signatures, access rules, and managing 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 78.

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 191.

If workspace is enabled, the ADOM must be locked before changes can be made. See Locking an ADOM on page 56.
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 58.



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: *Display Options*, *Find Unused Objects*, or *Find Duplicate Objects*.
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: *Display Options*, *Find Unused Objects*, or *Find Duplicate Objects*.

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 check box beside the option name. To turn off an option, clear the check box beside the option name. You can turn on all of the options in a category by selecting the check box beside the category name. For example, you can turn on all firewall objects by selecting the check box 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.

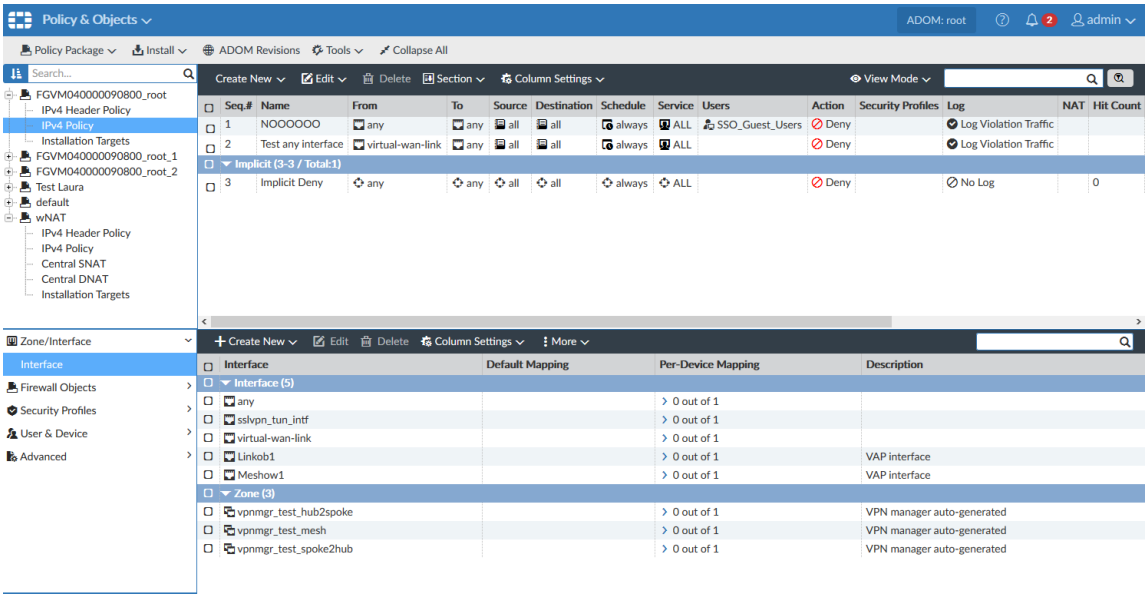
Once turned on, you can configure the corresponding options from the appropriate location on the *Policy & Objects* > *Object Configurations* pane.

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.



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.

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* check box 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.
4. Enter a name for the new policy package.
5. (Optional) Click the *In Folder* button to select a folder.
6. (Optional) Select the *Central NAT* check box to enable *Central SNAT* and *Central DNAT* policy types.
7. Click *OK* to add the policy package.

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.

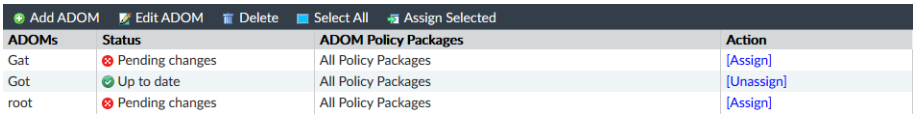
Assign a global policy package

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.

To assign a global policy package:

1. Ensure you are in the *Global* ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package, click *Assignment*. The ADOM assignment list is displayed in the content pane.



4. If required, select *Add ADOM* to add an ADOM to the assignment list.
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, 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.

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.

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. From the *Install* 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 Install wizard on page 116. For more information on editing the installation targets, see Policy package installation targets on page 198.

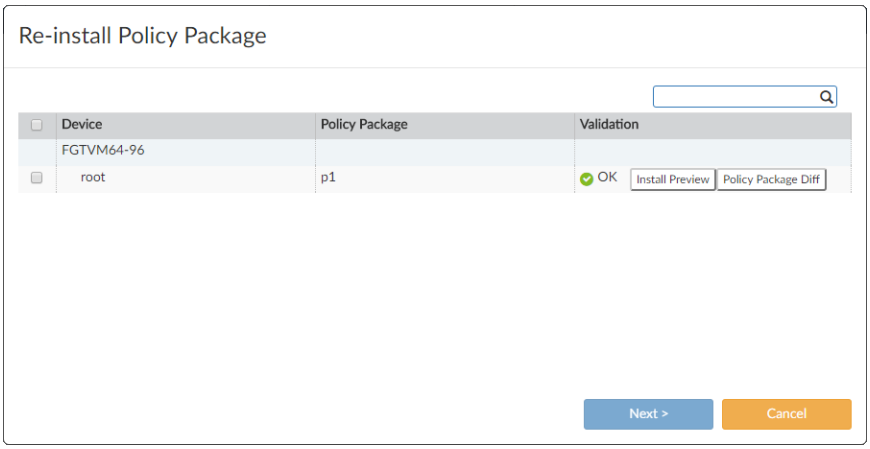
Reinstall a policy package

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

To reinstall a policy package to a target device:

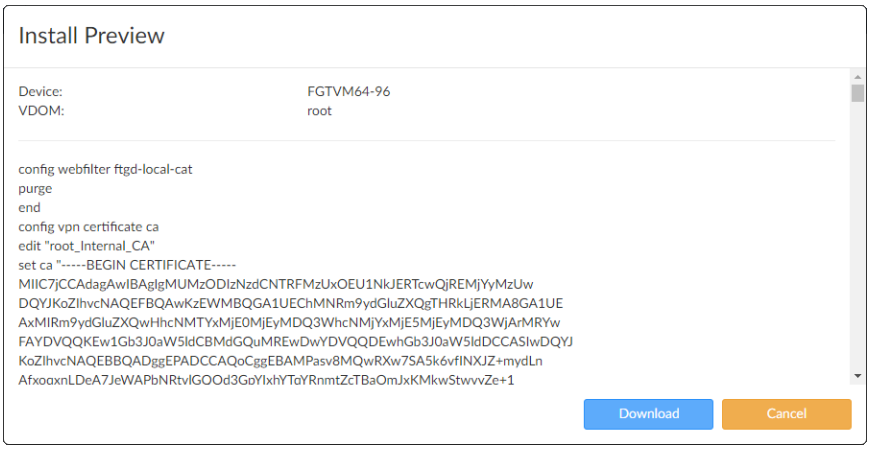
1. Ensure you are in the ADOM that contains the policy package.
2. Perform one of the following actions:
   - Go to *Policy & Objects* > *Policy Packages*, and select a policy package.
   - Go to *Device Manager*, and select a device.
3. In the toolbar, select *Install* > *Re-install Policy*.

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



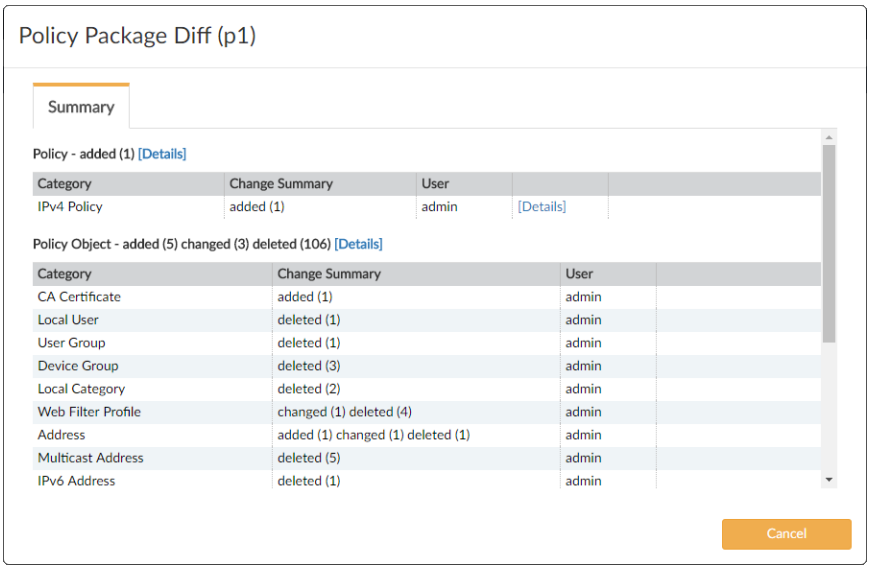
4. (Optional) View a preview of the installation.
   a. Click the *Install Preview* button.

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



   b. Click the *Download* button to download a text file of the preview information.
   c. Click the *Cancel* button to close the page and return to the wizard.
5. (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 *Cancel* to close the page and return to the wizard.
6. Click *Next*.
7. 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. Click *Schedule Install*, and set the install schedule date and time.
5. Click *Next*. In the device selection screen, edit the installation targets as required.
6. Click *Next*. In the interface validation screen, edit the interface mapping as required.
7. Click *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. Click *Cancel Schedule* to cancel the install schedule, then click *OK* in the confirmation dialog box to cancel the schedule. Otherwise, edit the install schedule as required and click *OK* to save your changes.

Export a policy package

You can export a policy package to a 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, and from the *Policy Package* menu, select *Export*.
   Policy packages are exported as CSV files.

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.

Config Status	Icon	Description
Modified (recent auto-updated)	Yellow triangle	Configurations are modified on FortiManager and configurations modified on the managed device are auto synced to FortiManager.
Out of Sync	Red X	Configurations are modified on the managed device and not synced to FortiManager.
Conflict	Red X	When one of the following happens: • Install failed • Configurations are modified on both FortiManager and the managed device, and not auto synced to FortiManager.
Unknown	Gray question mark	When one of the following happens: • Connection goes down • No revision is generated, like added model device

The following table identifies the different available policy package statuses.

Policy Package Status	Icon	Description
Imported	Green check	Policies and objects are imported into FortiManager.
Synchronized	Green check	Policies and objects are synchronized between FortiManager and the managed device.
Modified	Yellow triangle	Policies or objects are modified on FortiManager.
Out of Sync	Red X	Policies or objects are modified on the managed device.
Unknown with policy package name	Gray question mark	Configurations of the managed device are retrieved on FortiManager after being imported/installed.
Never Installed	Yellow triangle	No policy package is imported or installed.

The following options are available:

Add	Click to add installation targets (device/group) for the policy package selected. Select each *Device/Group* to be added, then click *OK*.
Remove	Click to delete the selected entries from the installation target for the policy package selected.
Install	Select an entry in the table and, from the *Install* menu, select *Install Wizard* or *Re-install Policy*.
Search	Use the search field to search installation targets. Entering text in the search field will highlight matches.

Perform a policy consistency check

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

The check will verify:

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

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

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

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.

To view the results of the last policy consistency check:

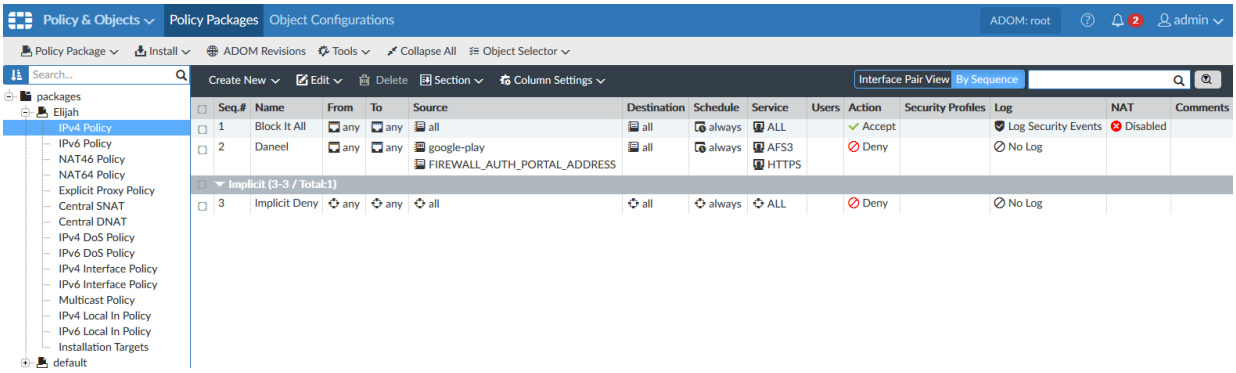
1. Select the ADOM for which you performed a consistency check.
2. Go to *Policy & Objects* > *Policy Packages*.
3. Select a policy package or folder, and from the *Policy Package* menu, select *Policy Check*. The *Policy Consistency Check* dialog box opens.
4. To view the results of the most recent 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.

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. 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. In the following example, the *default* policy package is displayed with its policies, such as IPv4 Policy, IPv6 Policy, and so on. The policies that are displayed for each policy package are controlled by the display options. See Display options on page 191 for more information.



You can configure the following policies for a policy package:

IP policies	Central SNAT	Interface policy
NAT policies	Central DNAT	Multicast policy
Explicit proxy policy	DoS policy	Local in policy

Various options are also available from column specific right-click menus, for more information see Column options on page 201.

For more information about policies, see the *FortiOS Handbook,* available in the Fortinet Document Library.

If workspace or workflow is enabled, the ADOM must be locked before changes can be made. See Locking an ADOM on page 56.

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

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 drop-down 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 view the hit count for each policy in a policy package. You must enable policy hit counts before you can view the tally.

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* column.

Creating policies

To create a new policy:

Policy creation varies depending on the type of policy that is being created. See the section below 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.

For information on creating policies, see the *FortiOS Handbook*, available in the Fortinet Document Library.

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 204 and Drag and drop objects on page 204.

The right-click menu changes based on the cell or object that is clicked on.

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 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:

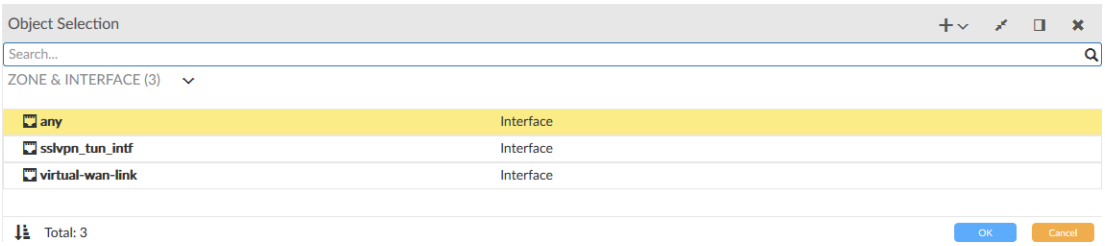
You can use sections to help organize your policy list. Policies can also be appended to sections.

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 191.



Create New	Click the create new drop-down list, then select the object type, to make a new object. See Create a new object on page 231.
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.
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 Selector* frame.

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 233 and Clone an object on page 234.

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.

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*.
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
5. click *OK* to save the service. The custom service will be added to the available services.

Name	Edit the service name as required.
Comments	Type an optional comment.
Service Type	Select *Firewall* or *Explicit Proxy*.
Show in service list	Select to display the object in the services list.
Category	Select a category for the service.
Protocol Type	Select the protocol from the drop-down list. Select one of the following: *TCP/UDP/SCTP*, *ICMP*, *ICMP6*, or *IP*.
IP/FQDN	Type the IP address or FQDN. This menu item is available when *Protocol* is set to *TCP/UDP/SCTP*. You can then define the protocol, source port, and destination port in the table.
Type	Type the service type in the text field. This menu item is available when *Protocol* is set to *ICMP* or *ICMP6*.
Code	Type the code in the text field. This menu item is available when *Protocol* is set to *ICMP* or *ICMP6*.
Protocol Number	Type the protocol number in the text field. This menu item is available when *Protocol Type* is set to *IP*.
Advanced Options	For more information on advanced option, see the *FortiOS CLI Reference*.
check-reset-range	Configure ICMP error message verification. • `disable`: The FortiGate unit does not validate ICMP error messages. • `strict`: If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) | TCP(C,D) header, then if FortiManager can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If it is enabled, the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the `anti-replay` option checks packets. • `default`: Use the global setting defined in `system global`. This field is available when `protocol` is `TCP/UDP/SCTP`. This field is not available if `explicit-proxy` is enabled.
Color	Click the icon to select a custom, colored icon to display next to the service name.

	session-ttl	Type the default session timeout in seconds. The valid range is from 300 - 604 800 seconds. Type `0` to use either the `per-policy session-ttl` or `per-VDOM session-ttl`, as applicable. This is available when `protocol` is `TCP/UDP/SCTP`.
	tcp-halfclose-timer	Type how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is from 1 to 86400 seconds. Type `0` to use the global setting defined in `system global`. This is available when `protocol` is `TCP/UDP/SCTP`.
	tcp-halfopen-timer	Type how many seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded. The valid range is from 1 to 86400 seconds. Type `0` to use the global setting defined in `system global`. This is available when `protocol` is `TCP/UDP/SCTP`.
	tcp-timewait-timer	Set the length of the TCP TIME-WAIT state in seconds. As described in RFC 793, the "...TIME-WAIT state represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request." Reducing the length of the TIME-WAIT state means the FortiGate unit can close terminated sessions faster, which means that more new sessions can be opened before the session limit is reached. The valid range is 0 to 300 seconds. A value of 0 sets the TCP TIME-WAIT to 0 seconds. Type `0` to use the global setting defined in `system global`. This is available when `protocol` is `TCP/UDP/SCTP`.
	udp-idle-timer	Type the number of seconds before an idle UDP connection times out. The valid range is from 1 to 86400 seconds. Type `0` to use the global setting defined in `system global`. This is available when `protocol` is `TCP/UDP/SCTP`.

To edit a policy action:

1. Select desired policy type in the tree menu.
2. Select the policy, and from the *Edit* menu, select *Edit*.
3. Set the *Action* option, and click *OK*.

To edit policy logging:

1. Select desired policy type in the tree menu.
2. Right-click the *Log* column, and select options from the menu.

To edit policy security profiles with dual pane disabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.

4. In the *Security Profiles* column, click the cell in the policy that you want to edit. The *Object Selector* frame is displayed.
5. In the *Object Selector* frame, locate the profiles, then drag and drop the object onto the cell in the *Security Profiles* column for the policy that you want to change.
6. Click *OK* to close the *Object Selector* frame.

To edit policy security profiles with dual pane enabled:

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

The policy action must be *Accept* to add security profiles to the policy.

IP policies

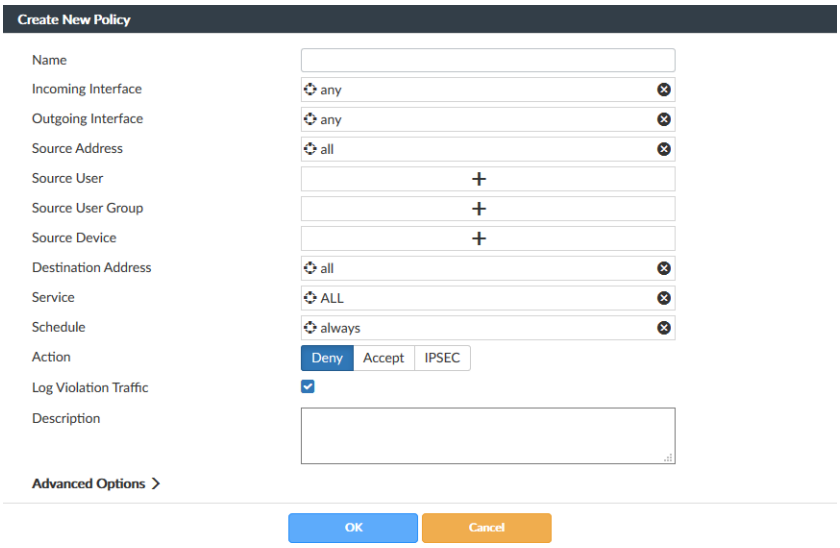
The section describes how to create new IPv4 and IPv6 policies.

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* check box 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.



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 *Object Selector* frame, or drag and drop the interface from the object pane. Select the remove icon to remove values. New objects can be created by clicking the *Create New* icon in the *Object Selector* frame. See Create a new object on page 231 for more information.
Outgoing Interface	Select outgoing interfaces.
Source Address	Select source addresses.
Source User	Select source users.
Source User Group	Select source user groups.
Source Device	Select source devices, device groups, and device categories.
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: *ACCEPT*, *DENY*, or *IPSEC*. *IPSEC* is not available for IPv6 policies.
Log Violation Traffic	Select to log violation traffic. This option is available when the *Action* is *DENY*.

Log Traffic	Select one of the following options: • *No Log* • *Log Security Events* • *Log All Sessions* When *Log Security Events* or *Log All Sessions* is selected, you can select to generate logs when the session starts and to capture packets. This option is available when the *Action* is *ACCEPT* or *IPSEC*.
NAT	Select to enable NAT. If enabled, select *Use Destination Interface Address* or *Dynamic IP Pool*, and select *Fixed Port* if required. If *Dynamic IP Pool* is selected, select pools. This option is available when the *Action* is *ACCEPT*.
VPN Tunnel	Select a VPN from the drop down list. Select to allow traffic to be initiated from the remote site. This option is available when the *Action* is *IPSEC*.
Security Profiles	Select to add security profiles or profile groups. This option is available when the *Action* is *ACCEPT* or *IPSEC*. The following profile types can be added: • 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 • CASI • Proxy Options • Profile Group (available when *Use Security Profile Group* is selected)
Shared Shaper	Select traffic shapers. This option is available if the *Action* is *ACCEPT* or *IPSEC*.
Reverse Shaper	Select traffic shapers. This option is available if the *Action* is *ACCEPT* or *IPSEC* and at least one forward traffic shaper is selected.
Per-IP Shaper	Select per IP traffic shapers. This option is available if the *Action* is *ACCEPT* or *IPSEC*.
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 below. For more information on advanced option, see the *FortiOS CLI Reference*.

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 drop-down list.	none
delay-tcp-npu-sessoin	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 `diffservcode-rev`.	disable
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
dsri	Enable or disable DSRI (Disable Server Response Inspection).	disable
dstaddr-negate	Enable or disable negated destination address match.	disable

Option	Description	Default
firewall-session-dirty	Packet session management, either *check-all* or *check-new*.	check-all
fsso	Enable or disable FSSO (IPv4 only).	disable
fsso-agent-for-ntlm	Select the FSSO agent for NTLM from the drop-down list (IPv4 only).	none
identity-based-route	Name of identity-based routing rule (IPv4 only).	none
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
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
redirect-url	URL redirection after disclaimer/authentication (IPv4 only).	none
replacemsg-override-group	Specify authentication replacement message override group.	none
rsso	Enable or disable RADIUS Single Sign-On.	disable
rtp-addr	Select the RTP address from the drop-down 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

Option	Description	Default
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
ssl-mirror	Enable or disable SSL mirror.	disable
ssl-mirror-intf	Mirror interface name.	none
tags	Applied object tags.	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
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
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
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
wsso	Enable or disable WiFi Single Sign-On (IPv4 only).	enable

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* check boxes 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 *Object Selector* frame, or drag and drop the interface 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: *ACCEPT*, or *DENY*.
Log Allowed Traffic	Select to log allowed traffic.
NAT	NAT is enabled by default for this policy type when the *Action* is *ACCEPT*. *Use Destination Interface Address* is selected by default. Select *Fixed Port* if required.
Traffic Shaping	Select traffic shapers. This option is available if the *Action* is *ACCEPT*.
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 *Action* is *ACCEPT*.
Description	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	
permit-any-host	Enable to accept UDP packets from any host.
tags	Applied object tags.
tcp-mss-receiver	Type a value for the receiver's TCP MSS.
tcp-mss-sender	Type a value for the sender's TCP MSS.

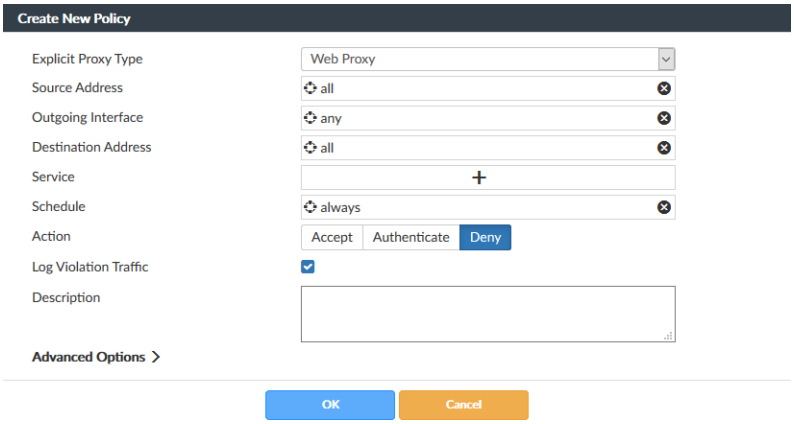
Explicit proxy policy

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

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

To create a new explicit 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 from the drop-down list: *Web Proxy*, *FTP Proxy*, or *WAN Opt Proxy*.

Source Address	Select source addresses from the *Object Selector* frame, or drag and drop the address from the object pane.
Outgoing Interface	Select outgoing interfaces.
Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
Service	Select services and service groups. This option is only available when the proxy type is set to *Web Proxy* or *WAN Opt Proxy*.
Schedule	Select schedules, one time or recurring, and schedule groups. This option is not available when the *Action* is *Authenticate*.
Action	Select an action for the policy to take: *Accept*, *Authenticate*, or *Deny*.
Log Traffic	Select one of the following options: • *No Log* • *Log Security Events* • *Log All Sessions* When *Log All Sessions* is selected, you can select to generate logs when the session starts. This option is available when the *Action* is *Accept*.
Log Violation Traffic	Select to log violation traffic. This option is available when the *Action* is *Deny*.
Disclaimer Options	Set the Display Disclaimer: *Disable*, *By Domain*, *By Policy*, or *By User*. These options are available when the *Action* is *Accept*.
Security Profiles	Select to add security profiles or profile groups. This option is available when the *Action* is *ACCEPT* or *IPSEC*. The following profile types can be added: • Antivirus • Web Filter • Application Control • CASI • IPS • DLP Sensor • ICAP • Web Application Firewall • Proxy Options • SSL/SSH Inspection • Profile Group (available when *Use Security Profile Group* is selected) This option is available when the *Action* is *Accept*.

Web Cache	Select to turn on web cache. This option is available when the *Action* is *Authenticate*.
Web Proxy Forwarding Server	Select a web proxy forwarding server from the drop-down list. This option is not available when the *Action* is *Deny*.
Description	Add a description of the policy, such as its purpose, or the changes that have been made to it.
User Authentication Options	Configure authentication rules. See Authentication rules on page 218 for information. This option is available when the *Action* is *Authenticate*.
IP Based Authentication	Enable or disable IP based authentication. When enabled, select the single sign-on method from the drop-down list: *FSSO* or *RSSO*. This option is available when the *Action* is *Authenticate*.
Default Authentication Method	Select the default authentication method: *None*, *Basic*, *Digest*, *NTLM*, or *Form-based*. This option is available when the *Action* is *Authenticate*.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the *FortiOS CLI Reference*.

Advanced options

Option	Description	Default
comments	Add comments.	none
dstaddr-negate	Enable or disable negated destination address match.	disable
dstaddr6	Select an IPv6 firewall address from the drop-down list.	none
global-label	Enter a global label.	none
label	Enter a label	none
require-tfa	Enable or disable requiring 2-factor authentication.	disable
scan-botnet-connections	Enable or disable scanning of connections to Botnet servers.	disable
service-negate	Enable or disable negated service match.	disable
srcaddr-negate	Enable or disable negated source address match.	disable
srcaddr6	Select an IPv6 firewall address from the drop-down list.	none
tags	Applied object tags.	none

Option	Description	Default
transaction-based	Enable or disable transaction based authentication.	disable
transparent	Use IP address of client to connect to server.	disable
web-auth-cookie	Enable or disable web authentication cookie.	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 drop-down list.	none

Authentication rules

Authentication rules can be added, edited, and deleted as required.

To add an authentication rule:

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, if applicable, from the *Create New* menu select *Insert Above* or *Insert Below*. The *Create New Policy* pane opens.
4. Select *Authentication* as the *Action*.
5. In the *User Authentication Options* section, click *Create New* in the table toolbar. The *Create New Identity Policy* dialog box opens.
6. Configure the options as required, then click *OK* to create the rule.

To edit an authentication rule:

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, if applicable, from the *Create New* menu select *Insert Above* or *Insert Below*. The *Create New Policy* pane opens.
4. Select *Authentication* as the *Action*.
5. In the *User Authentication Options* section, select the rule that needs to be edited, then click *Edit* in the table toolbar. The *Edit Identity Policy* dialog box opens.
6. Configure the options as required, then click *OK* to apply your changes.

To delete an authentication rule or rules:

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, if applicable, from the *Create New* menu select *Insert Above* or *Insert Below*. The *Create New Policy* pane opens.
4. Select *Authentication* as the *Action*.

5. In the *User Authentication Options* section, select the rule or rules that need to be deleted, then click *Delete* in the table toolbar.
6. Click *OK* in the confirmation dialog box to delete the selected rule or rules.

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 193.

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:

Original Address	Select the original address from the *Object Selector* frame, or drag and drop the address from the object pane.
Destination Address	Select the destination address.
IP Pool	Select the IP pool.
Protocol	Enter the protocol number, from 0 to 255.

Original Port	Enter the original port number, from 0 to 65535.
NAT Port	Enter the NAT port number, from 0 to 65535.

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 193.

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: *Static NAT*, *DNS Translation*, or *FQDN*.
	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 *FQDN*.
	Mapped IP Address/Range	Enter the mapped IP address. This option is not available when the network type is *FQDN*.
	External IP Address	Enter the external IP address. This option is only available when the network type is *FQDN*.
	Mapped Address	Select the mapped address. This option is only available when the network type is *FQDN*.
	Source Interface Filter	Select a source interface filter.
Source Address Filter		Enable or disable source address filters. When enabled, multiple filters can be added using the *Add* icon.
Port Forwarding		Enable or disable port forwarding.
	Protocol	Select the protocol: *TCP*, *UDP*, *SCTP*, or *ICMP*.
	External Service Port	Enter the external service port. This option is not available when *Protocol* is *ICMP*.
	Map to Port	Enter the map to port. This option is not available when *Protocol* is *ICMP*.
Enable ARP Reply		Select to enable ARP reply.
Advanced Options		Configure advanced options, see Advanced options below. For more information on advanced option, see the *FortiOS CLI Reference*.
Per-Device Mapping		If multiple imported VIP objects have the same name but different details, the object type will become Dynamic Virtual IP, and the per-device mappings will be listed here. Mappings can also be manually added, edited, and deleted as needed.

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
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
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

Option	Description	Default
outlook-web-access	If enabled, the `Front-End-Https: on` 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: • `high`: permit only high encryption algorithms: AES or 3DES. • `medium`: permit high or medium (RC4) algorithms. • `low`: permit high, medium, or low (DES) algorithms. • `custom`: only allow some preselected cipher suites to be used.	high
ssl-client-fallback	Enable to prevent Downgrade Attacks on client connections.	enable
ssl-client-renegotiation	Select the SSL secure renegotiation policy. • `allow`: allow, but do not require secure renegotiation. • `deny`: do not allow renegotiation. • `secure`: require secure renegotiation.	allow
ssl-client-session-state-max	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`: expire SSL session states when either `ssl-client-session-state-max` or `ssl-client-session-state-timeout` is exceeded, regardless of which occurs first. • `count`: expire SSL session states when `ssl-client-session-state-max` is exceeded. • `disable`: expire all SSL session states. • `time`: expire SSL session states when `ssl-client-session-state-timeout` is exceeded.	both
ssl-dh-bits	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-http-location-conversion	Enable to replace http with https in the reply's Location HTTP header field.	disable

Option	Description	Default
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: `ssl-3.0`, `tls-1.0`, `tls-1.1`, or `tls-1.2`.	tls-1.2
ssl-min-version	The lowest version of SSL/TLS to allow in SSL sessions: `ssl-3.0`, `tls-1.0`, `tls-1.1`, or `tls-1.2`.	tls-1.0
ssl-pfs	Select the handling of Perfect Forward Secrecy (PFS) by controlling the cipher suites that can be selected. • `allow`: allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected. • `deny`: allow only non-Diffie-Hellman cipher-suites, so PFS is not applied. • `require`: allow only Diffie-Hellman cipher-suites, so PFS is applied.	allow
ssl-send-empty-frags	Enable to precede the record with empty fragments to thwart attacks on CBC IV. Disable this option if SSL acceleration will be used with an old or buggy SSL implementation which cannot properly handle empty fragments.	enable
ssl-server-algorithm	Set the permitted encryption algorithms for SSL server sessions according to encryption strength: • `high`: permit only high encryption algorithms: AES or 3DES. • `medium`: permit high or medium (RC4) algorithms. • `low`: permit high, medium, or low (DES) algorithms. • `custom`: only allow some preselected cipher suites to be used.	client
ssl-server-max-version	The highest version of SSL/TLS to allow in SSL server sessions: `client`, `ssl-3.0`, `tls-1.0`, `tls-1.1`, or `tls-1.2`.	client
ssl-server-min-version	The lowest version of SSL/TLS to allow in SSL server sessions: `client`, `ssl-3.0`, `tls-1.0`, `tls-1.1`, or `tls-1.2`.	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

Option	Description	Default
ssl-server-session-state-type	The method to use to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate. • `both`: expire SSL session states when either `ssl-client-session-state-max` or `ssl-client-session-state-timeout` is exceeded, regardless of which occurs first. • `count`: expire SSL session states when `ssl-client-session-state-max` is exceeded. • `disable`: expire all SSL session states. • `time`: expire SSL session states when `ssl-client-session-state-timeout` is exceeded.	both
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 policy

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* check boxes to display these option.

To create a DoS policy:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Policy Packages*.
3. In the tree menu for the policy package, click *IPv4 DoS Policy* or *IPv6 DoS Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.
5. Configure the following settings, then click *OK* to create the policy:

Incoming Interface	Select the incoming interface from the *Object Selector* 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.

Interface policy

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 *Object Selector* 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: *No Log*, *Log Security Events*, or *Log All Sessions*.
AntiVirus Profile	Select to enable antivirus and select the profile from the drop-down list.
Web Filter Profile	Select to enable Web Filter and select the profile from the drop-down list.
Application Control	Select to enable Application Control and select the profile from the drop-down list.
IPS Profile	Select to enable IPS and select the profile from the drop-down list.
Email Filter Profile	Select to enable Email Filter and select the profile from the drop-down list.
DLP Sensor	Select to enable DLP Sensor and select the profile from the drop-down list.
Advanced Options	
casi-profile	Select a casi profile from the drop-down list.
casi-profile-status	Enable or disable casi-profile-status.
dsri	Enable or disable dsri.
scan-botnet-connections	Enable or disable scanning of connections to Botnet servers.

Multicast policy

Multicasting consists of using a single source to send data to many receivers simultaneously, while conserving bandwidth and reducing network traffic. For information about multicasting, see the *FortiOS Handbook* available in the Fortinet Document Library.

On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *Mulitcast Policy* check box 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 *Object Selector* frame, or drag and drop the interface from the object pane. If no multicast interfaces are configured, click the *Create New Object* button to open the *Create New Dynamic Multicast Interface* 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	Select 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 drop-down list: *ANY*, *ICMP*, *IGMP*, *TCP*, *UDP*, *OSFP*, or *Others*.
Port Range	Set the port range. This option is only available when *Protocol Option* is *TCP* or *UDP*.
Protocol Number	Enter the protocol number, from 1 to 256. This option is only available when *Protocol Option* is *Others*.
Log Traffic	Select to log traffic.
Advanced Options	Enable or disable *auto-asic-offload*, and enter the *id* number.

Local in policy

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* check boxes 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: *ACCEPT*, *DENY*, or *IPSEC*. *IPSEC* is not available for IPv6 policies.
HA Management Interface Only	Select to enable. This option is only available for IPv4 policies.

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.

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 191.

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 pane, and dropping them in cells in the policy. For more information see Drag and drop objects on page 204.

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

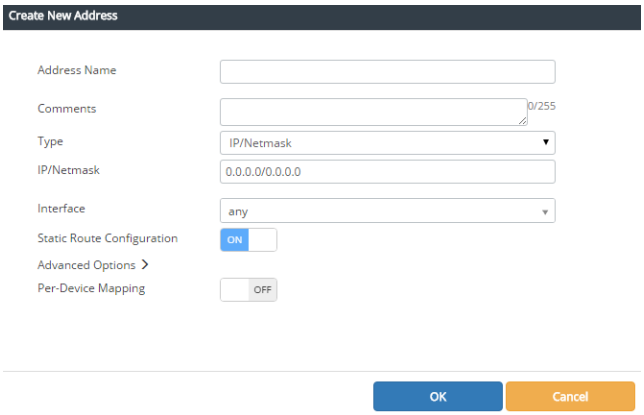
Create a new object

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 *New Address* dialog box opens.



In 5.2.0 or later, 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, and click *OK* to create the new object.

Map a dynamic object

The devices and VDOMs to which a global object is mapped can also be viewed from the object list. In 5.2 or later, 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 143

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 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, and select *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 *Managed on ADOM* check box, the FortiManager ADOM manages members for the object, and you must specify members for the object. When you clear the *Manage on ADOM* check box, 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*.

   You can delete the object, even when the object is used by a policy. After you delete the object, the policy is updated to replace the IP address for the object with the word *None*.

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.

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, and click *Edit*.
5. Edit the information as required, then 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*.

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.

Find unused objects

You can 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*.

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*.

CLI-Only objects

FortiManager 5.2.0 or later adds the ability to configure objects in the GUI which are available only via the FortiOS command line interface.

FortiToken configuration example

To configure FortiToken objects for FortiToken management:

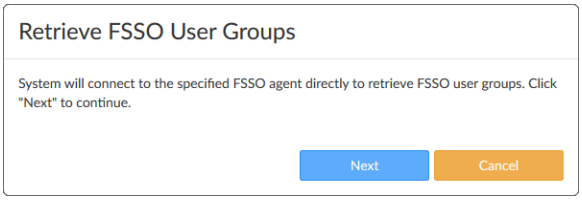
1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Object Configurations*.
3. Go to *User & Device* > *FortiTokens*.
4. Click *Create New*.
5. Type the serial number or serial numbers of the FortiToken unit or units and click *OK*. Up to ten serial numbers can be entered.
6. Go to *User & Device* > *User Definition* to create a new user.
7. When creating the new user, select *FortiToken*, and then select the FortiToken from the drop down 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.

To get groups from FSSO:

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



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

To get groups from an LDAP server:

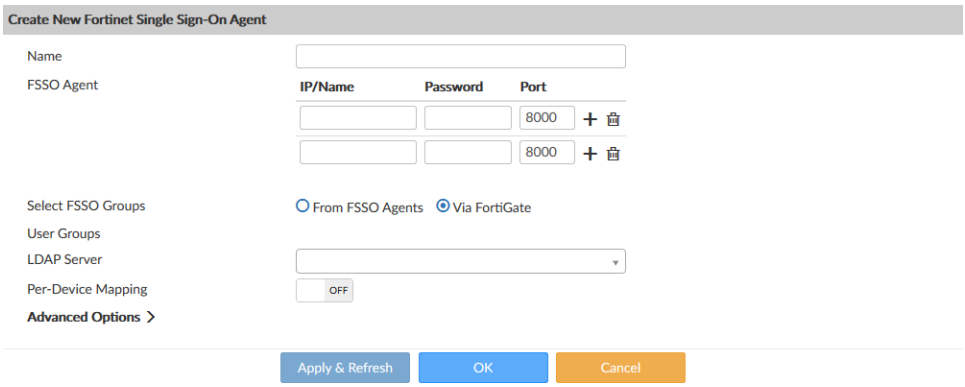
1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* > *Object Configurations*. and select *User & Device* > *Single Sign-On*.
3. Click *Create New* > *Fortinet Single Sign-On Agent* from the drop-down list.
4. Enter a unique name for the agent in the *Name* field.
5. Select an LDAP server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

   You can also select *Manually Specify* in the *Select LDAP Groups* field, and then manually enter the group names.
7. Select *OK*.

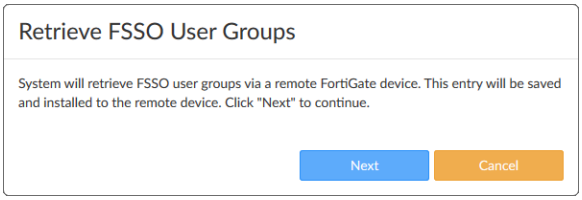
To get groups via a remote FortiGate:

The FortiGate device configuration must be synchronized or retrieving the FSSO user groups will fail. See Checking device configuration status on page 127.

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



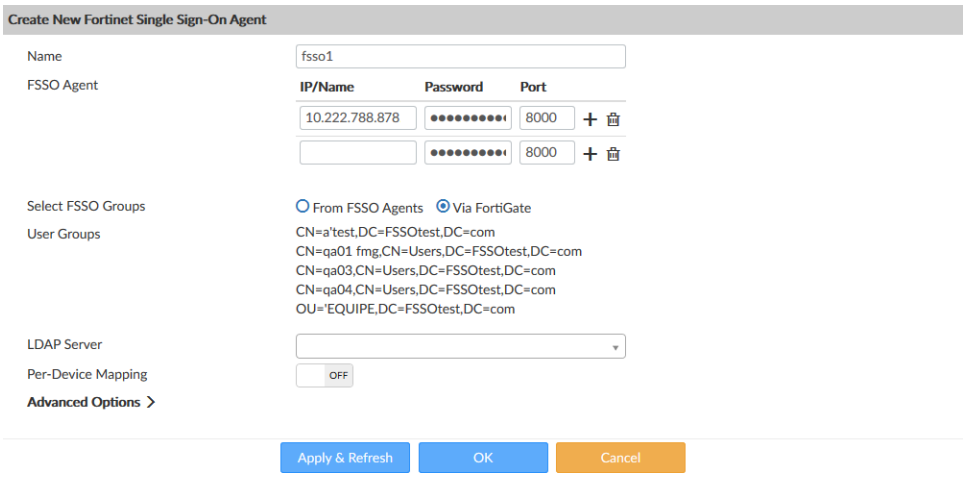
3. Enter a unique name for the agent in the *Name* field.
4. Enter the IP address or name, password, and port number of the FSSO servers in the FSSO Agent field. Add and remove servers as needed by clicking the *Add* and *Remove* icons at the end of the rows.
5. Select *Via FortiGate* in the *Select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



7. Click *Next* to proceed with the wizard.

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

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



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

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

To get groups from AD:

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

   You can also select *Manually Specify* in the *Select LDAP Groups* field, and then manually enter the group

names.

7. Select *OK*.

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 *Lock this revision from auto deletion.*
Created by	The administrator that created the ADOM revision.
Created Time	The ADOM revision creation date and time.
Comment	Optional comments typed in the *Description* field when the ADOM revision was created.

The following options are available:

Create New	Select to create a new ADOM revision.
Edit	Right-click on a revision in the table and select *Edit* in the menu to edit the ADOM revision.
Delete	Right-click on a revision in the table and select *Delete* in the menu to delete the ADOM revision. When *Lock this revision from auto deletion* is selected, you are not able to delete the ADOM revision.
Restore	Right-click on a revision in the table and select *Restore* in the menu to restore the ADOM revision. Restoring a revision will revert policy packages, objects and VPN console to the selected version. Select *OK* to continue.
More > Lock Revision	Right-click on a revision in the table and select *Lock* from the *More* menu to lock this revision from auto deletion.

More > Unlock Revision	Right-click on a revision in the table and select *Unlock* from the *More* menu to unlock this revision. When the ADOM revision is in an unlocked state, auto deletion will occur in accordance with your auto deletion settings.
View Revision Diff	Right-click on a revision in the table and select *View Revision Diff* in the menu. The Summary page will be displayed. This page shows the revision differences between the selected revision and the current database.
Settings	Select to configure the automatic deletion settings for ADOM revisions.
Close	Select to close the *ADOM Revision* dialog box and return to the *Policy & Objects* tab.

To create a new ADOM revision:

1. Go to *Policy & Objects*, and click *ADOM Revisions*. The *ADOM Revision* dialog box opens.
2. Click *Create New*. The *Create New Revision* dialog box opens.
3. Type a name for the revisions in the *Name* field.
4. Optionally, type a description of the revision in the *Description* field.
5. To prevent the revision from being automatically deleted, select *Lock this revision from auto deletion*.
6. Click *OK* to create the new ADOM revision.

To edit an ADOM revision:

1. Open the *ADOM Revisions* dialog box.
2. Select a revision, and click *Edit*. The *Edit Revision* dialog box opens.
3. Edit the revision details as required, then click *OK* to apply your changes.

To delete ADOM revisions:

1. Open the *ADOM Revisions* dialog box.
2. Select a revision, and click *Delete*.
   You can select multiple revisions by selecting the check box 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.

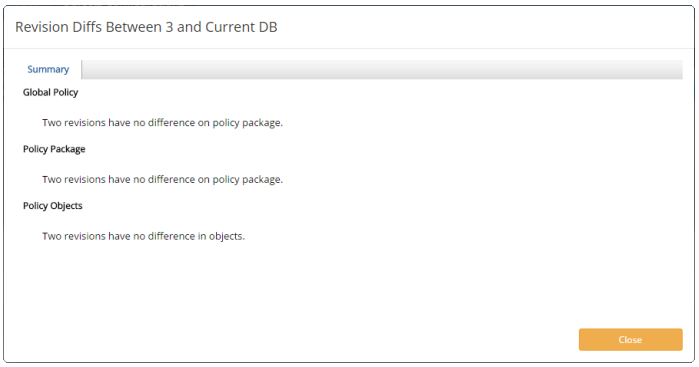
   The *Restore Revision* dialog box opens. Restoring a revision will revert policy packages, objects and VPN console to the selected version.
4. Click *OK* to continue.

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* check box 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.

VPN Manager

Use the *VPN Manager* pane to enable and use central VPN management. You can view and configure IPsec VPN and SSL-VPN settings that you can install to one or more devices.

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.
SSL-VPN	Create, monitor, and manage SSL-VPN settings. You can also create, edit, and delete portal profiles for SSL-VPN settings.

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.

Following is an overview of how to use central VPN management to configure and install IPsec VPN settings to multiple devices. An overview of configuring and installing SSL-VPN settings is also included.

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.

To create IPsec VPN settings:

1. Enable central VPN management. See Enabling central VPN management on page 242.
2. Create a VPN community, which is sometimes called a VPN topology. See Create IPsec VPN communities on page 243.
3. Create a managed gateway. See Create a VPN managed gateway on page 250.

To create SSL-VPN settings:

1. Create custom profiles. See Create SSL-VPN portal profiles on page 256.

   Alternately, you can skip this step, and use the default portal profiles. See Default SSL-VPN portal profiles on page 255.
2. Add an SSL VPN to a device, and select a portal profile. See Add SSL-VPN on page 254.

To install VPN objects to devices:

1. Plan the VPN security policies. See VPN security policies on page 259.
2. In a policy package, create VPN security policies, and select the VPN settings. See Creating policies on page 202.
3. Edit the installation targets for the policy package to add all of the devices to which you want to install the VPN settings that are defined in the policy. 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 also enable centralized VPN management by using the *System Settings* > *Dashboard* pane.

Regardless of how you enable centralized VPN management, you use the *VPN Manager* > *IPsec VPN* pane for centralized VPN management.

To enable:

1. Go to *VPN Manager* > *IPsec VPN*.
2. Select *Enable*.
3. Click *OK* in the confirmation dialog box.

To enable 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. Beside *Central Management*, select the *VPN* check box.
5. Click *OK*. Centralized VPN management is enabled for the ADOM.

To enable when ADOMs disabled:

1. Go to *System Settings* > *Dashboard*.
2. Beside *VPN Management Mode*, select *Change VPN Management Mode*. The *Change VPN Management Mode* dialog box is displayed.
3. Click *OK*.

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.

Create IPsec VPN communities

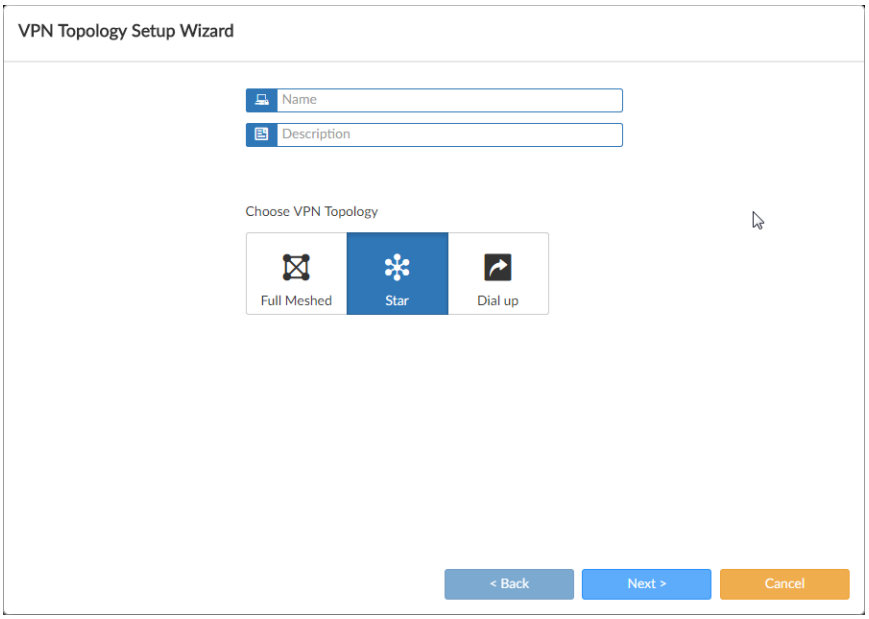
You can create one or more IPsec VPN communities. An IPsec VPN community is also sometimes called a VPN topology. A *VPN Topology Wizard* is available to help you set up topologies.

After you create the IPsec VPN community, you can create the VPN gateway. See IPsec VPN gateways on page 250.

To create a new IPsec VPN community:

1. Go to the *VPN Manager* > *IPsec VPN* tab.
2. From the *VPN Community* menu, select *Create New*.
   Alternately, you can click *Create New* in the toolbar.

   The VPN Topology Setup Wizard is displayed.



3. Complete the following options, and click *Next*.
   a. In the *Name* box, type a name for the VPN topology.
   b. In the *Description* box, type a description.
   c. Choose a topology by clicking *Full Meshed*, *Star*, or *Dial up*, and click *Next*.
      The next screen in the wizard is displayed.
4. Set the options, and click *Next*, until you complete all options in the wizard, and the *Summary* page is displayed.
   For a description of the options, see VPN Topology Setup Wizard reference on page 244.
5. On the *Summary* page, review the options, and click *OK*.

Once you have created your VPN topology, you can select to create a new managed gateway or external gateway for the topology.

VPN Topology Setup Wizard reference

The following table describes the options available in the VPN Topology Setup Wizard and on the Edit VPN Community page.

Name	Type a name for the VPN topology.
Description	Type an optional description.
Choose VPN Topology	Choose a topology type. Select one of: • *Full Meshed*: Each gateway has a tunnel to every other gateway. • *Star*: Each gateway has one tunnel to a central hub gateway. • *Dial up*: Some gateways, often mobile users, have dynamic IP addresses and contact the gateway to establish a tunnel.
Authentication	Select *Certificates* or *Pre-shared Key*. When you select *Pre-shared Key*, FortiGate implements the Encapsulated Security Payload (ESP) protocol. Internet Key Exchange (IKE) is performed automatically based on pre-shared keys or X.509 digital certificates.
Certificates	If you selected *Certificates*, select a certificate template. Fortinet provides several default certificate templates. You can also create certificate templates on the *Device Manager* > *Provisioning Templates* > *Certificate Templates* pane.
Pre-shared Key	If you selected *Pre-shared Key*, select *Generate* or *Specify*. When you select *Specify*, type the pre-shared key that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. You must define the same key at the remote peer or client. The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters. Alternatively, you can select to generate a random pre-shared key.
Encryption	Define the IKE Profile. Configure IKE Phase 1 and IKE Phase 2 settings.
IKE Security (Phase 1) Properties	Define the Phase 1 proposal settings .

Encryption Authentication	Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of three combinations. The remote peer or client must be configured to use at least one of the proposals that you define. Select one of the following symmetric-key encryption algorithms: • DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • 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. • 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. • ARIA128: A 128-bit block size that uses a 128-bit key. • ARIA192: A 128-bit block size that uses a 19- bit key. • ARIA256: A 128-bit block size that uses a 256-bit key. • SEED: A 16-round Feistel network with 128-bit blocks and a 128-bit key. Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations: • MD5: Message Digest 5, the hash algorithm developed by RSA Data Security. • SHA1: Secure Hash Algorithm 1, which produces a 160-bit message digest. • SHA256: Secure Hash Algorithm 2, which produces a 256-bit message digest. • SHA384: Secure Hash Algorithm 3, which produces a 384-bit message digest. • SHA512: Secure Hash Algorithm 3, which produces a 512-bit message digest. To specify a third combination, use the Add button beside the fields for the second combination.
IPsec Security (Phase 2) Properties	Define the Phase 2 proposal settings. When you define phase 2 parameters, you can choose any set of phase 1 parameters to set up a secure connection for the tunnel and authenticate the remote peer. Auto Key configuration applies to both tunnel-mode and interface-mode VPNs.

Encryption Authentication	Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of three combinations. The remote peer or client must be configured to use at least one of the proposals that you define. It is invalid to set both Encryption and Authentication to NULL. Select one of the following symmetric-key encryption algorithms: • NULL: Do not use an encryption algorithm. • DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • 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. • 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. • ARIA128: A 128-bit block size that uses a 128-bit key. • ARIA192: A 128-bit block size that uses a 19- bit key. • ARIA256: A 128-bit block size that uses a 256-bit key. • SEED: A 16-round Feistel network with 128-bit blocks and a 128-bit key Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations: • 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. To specify a third combination, use the Add button beside the fields for the second combination.
VPN Zone	Select to create VPN zones. When enabled, you can select to create default or custom zones. When disabled, no VPN zones are created.
Create Default Zones	Select to have default zones created for you.
Use Custom Zone	Select to choose what zones to create.

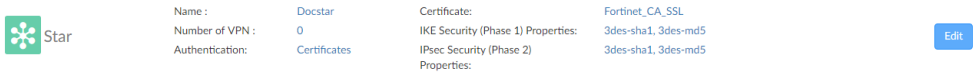
IKE Security Phase 1 Advanced Properties	
Diffie Hellman Group(s)	Select one or more of the following Diffie-Hellman (DH) groups: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21. At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations. Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.
Exchange Mode	Select either *Aggressive* or *Main (ID Protection)*. The FortiGate unit and the remote peer or dialup client exchange phase 1 parameters in either Main mode or Aggressive mode. This choice does not apply if you use IKE version 2, which is available only for route-based configurations. • In Main mode, the Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information • In Aggressive mode, the Phase 1 parameters are exchanged in single message with authentication information that is not encrypted. Although Main mode is more secure, you must select Aggressive mode if there is more than one dialup Phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier local ID). Descriptions of the peer options in this guide indicate whether Main or Aggressive mode is required.
Key Life	Type the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The keylife can be from 120 to 172800 seconds.
Dead Peer Detection	Select this check box to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required. You can use this option to receive notification whenever a tunnel goes up or down, or to keep the tunnel connection open when no traffic is being generated inside the tunnel. For example, in scenarios where a dialup client or dynamic DNS peer connects from an IP address that changes periodically, traffic may be suspended while the IP address changes.
IPsec Security Phase 2 Advanced Properties	
Diffie Hellman Group(s)	Select one or more of the following Diffie-Hellman (DH) groups: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21. At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations. Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.

Replay detection	Select to enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.
Perfect forward secrecy (PFS)	Select to enable or disable perfect forward secrecy (PFS). Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.
Key Life	Select the PFS key life. Select *Second, Kbytes,* or *Both* from the drop-down list and type the value in the text field.
Autokey Keep Alive	Select to enable or disable autokey keep alive. The phase 2 SA has a fixed duration. If there is traffic on the VPN as the SA nears expiry, a new SA is negotiated and the VPN switches to the new SA without interruption. If there is no traffic, the SA expires and the VPN tunnel goes down. A new SA will not be generated until there is traffic. The Autokey Keep Alive option ensures that a new SA is negotiated even if there is no traffic so that the VPN tunnel stays up.
Auto-Negotiate	Select to enable or disable auto-negotiation.
NAT Traversal	Select the check box 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 you enabled NAT traversal, type a keep-alive frequency setting (10-900 seconds).
Advanced-Options	For more information on advanced options, see the *FortiOS 5.2 CLI Reference*.
DPD	Select to enable or disable DPD. You can also choose to set to *on-demand* or *on-idle.*,
fcc-enforcement	Select to enable or disable FCC enforcement.
ike-version	Select the version of IKE to use. This is available only if IPsec Interface Mode is enabled. For more information about IKE v2, refer to RFC 4306. IKE v2 is not available if *Exchange Mode* is *Aggressive*. When IKE Version is set to 2, Mode and XAUTH are not available.
inter-vdom	Select to enable or disable the inter-vdom setting.

loccalid-type	Select the local ID type from the drop-down list. Select one of: • auto: Select type automatically • fqdn: Fully Qualified Domain name • user-fqdn: User Fully Qualified Domain Name • keyid: Key Identifier ID • address: IP Address • asn1dn: ASN.1 Distinguished Name
negotiate-timeout	Type the negotiation timeout value. The default is 30 seconds.

View IPsec VPN communities

You can view a quick status bar of settings for each VPN community without opening the VPN community for editing.



To view IPsec VPN communities:

1. Go to *VPN Manager* > *IPsec VPN*.
2. Click the *All VPN Communities* list. The list of communities is displayed.
3. Perform one of the following actions:
   - In the *All VPN Communities* list, select a community. A quick status bar for the selected community is displayed.
   - Click the *All VPN Communities* list. The list of communities is displayed.

Edit IPsec VPN communities

To edit IPsec VPN communities:

1. Go to *VPN Manager* > *IPsec VPN*.
2. In the *All VPN Communities* list, select a community.
   A quick status bar for the selected community is displayed.
3. Perform one of the following actions:
1. In the quick status bar, click *Edit*.
2. From the *VPN Community* menu, select *Edit*.

The *Edit VPN Community* page is displayed.

4. Edit the options, and click *OK*.
   For a description of the options, see VPN Topology Setup Wizard reference on page 244.

Monitor IPsec VPN communities

To monitor IPsec VPN communities:

1. Go to *VPN Manager* > *IPsec VPN* > *Monitor*.
2. Right-click a device, and select *Refresh*, *Bring Tunnel Up* or *Bring Tunnel Down*.

Manage IPsec VPN communities

You can manage IPsec VPN communities from the *VPN Manager* > *IPsec VPN* pane. Some options are available in the menu on the toolbar. Some options are available in the right-click menu. Right-click an IPsec VPN community to display the menu.

Option	Description
VPN Community	Select to display a menu where you can choose to create a new VPN community, edit a selected VPN community, or delete a selected VPN community.
Install Wizard	Launch the Install Wizard to install IPsec VPN settings to devices.
Create New	Create a new VPN community .
Edit	Edit the selected VPN community.
Delete	Delete the selected VPN community.
Config Gateways	Select to display a pane that lets you create managed and external gateways.
Add Managed Gateway	Select to start the VPN Gateway Setup Wizard.
Column Settings	In the *Column Settings* menu, select the column names that you want to display, and deselect the column names that you want to hide. Column settings include the option to restore columns to their default state.

IPsec VPN gateways

Once you have created the IPsec VPN topology, you can create a managed or external gateway. The settings on these pages are dependent on the VPN topology selected.

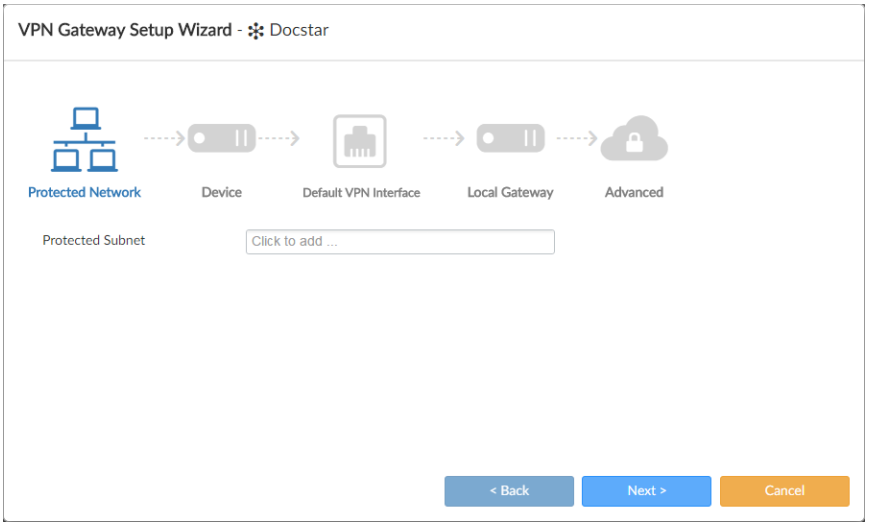
Create a VPN managed gateway

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 Create a VPN external gateway on page 252.

To create a VPN managed gateway:

1. Go to *VPN Manager* > *IPsec VPN*.
2. In the *All VPN Communities* list, select a community.
3. In the toolbar, select *Create New* > *Managed Gateway*.
   The *VPN Gateway Setup Wizard* pane is displayed.



4. In the *Protected Subnet* list, select a subnet, and click *Next*.
5. In the *Device* list, select a device, and click *Next*.
6. In the *Default VPN Interface* list, select an interface, and click *Next*.
7. In the *Local Gateway* list, type the gateway IP address, and click *Next*.
8. Beside *Routing*, select *Manual (via Device Manager)* or *Automatic*.
9. Expand *Advanced Options*, and configure the following settings:

Local ID	Type the local ID.
Routing	Select *Manual* or *Automatic* routing. Manual routes through Device Manager.
Summary Network(s)	Select a network and it's priority. Click + to add a new row.
Advanced Options	For more information on advanced options, see the *FortiOS 5.2 CLI Reference*.
authpasswd	Type the XAuth client password for the FortiGate. This field is available when `xauthtype` is set to client.
authusr	Type the XAuth client user name for the FortiGate. This field is available when `xauthtype` is set to client.

authusrgrp	Select the authentication user group from the drop-down list. This field is available when xauthtype is set to auto, pap, or chap. When the FortiGate unit is configured as an XAuth server, type 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.
banner	Type the banner value. Specify a message to send to IKE Configuration Method clients. Some clients display this message to users. This is available if mode-cfg (IKE Configuration Method) is enabled.
dns-mode	Select either manual or auto from the drop-down list. • auto: Assign DNS servers in the following order: • Servers assigned to interface by DHCP. • Per-VDOM assigned DNS servers. • Global DNS servers. • manual: Use DNS servers specified in DNS Server 1, DNS Server 2 etc.
domain	Type the domain value.
public-ip	Type the public IP address value. Use this field to configure a VPN with dynamic interfaces. Define a `public-ip` value here, which is the dynamically assigned PPPoE address, which remains static and does not change over time.
route-overlap	Select *allow*, *use-new*, or *use-old*.
spoke-zone	Select a spoke zone from the list.
unity-support	Select either enable or disable from the drop-down list.
vpn-zone	Select a VPN zone from the list.

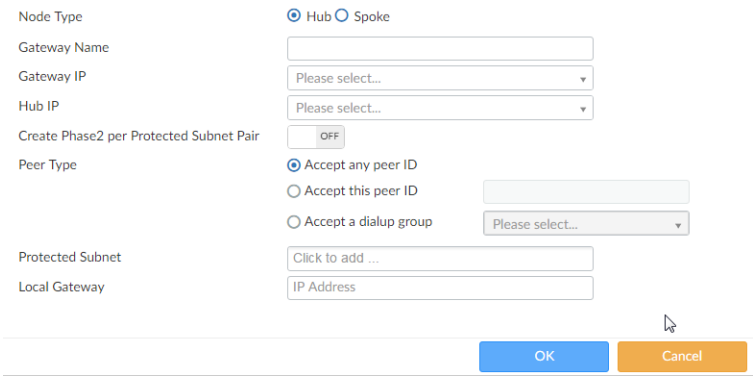
10. Click *OK* to save the settings.

Create a VPN external gateway

External gateways are not managed by FortiManager.

Create a VPN external gateway:

1. Go to *VPN Manager* > *IPsec VPN*.
2. In the *All VPN Communities* list, select a community.
3. In the toolbar, select *Create New* > *External Gateway*. The pane is displayed.



4. Configure the following settings:

Node Type	Select either *HUB* or *Spoke* from the drop-down list. This menu item is available when *Topology* is *Star* or *Dial up*.
Gateway Name	Type the gateway name.
Gateway IP	Select the gateway IP address from the drop-down list.
Hub IP	Select the hub IP address from the drop-down list. This menu item is available when *Topology* is *Star* or *Dial up* and *Node Type* is *HUB*.
Create Phase2 per Protected Subnet Pair	Select the checkbox to create a phase2 per protected subnet pair.
Routing	Select *Manual* or *Automatic* routing.
Peer Type	Select the peer type. Select one of the following: • Accept any peer ID • Accept this peer ID (type the peer ID in the text field) • Accept a dialup group (select the 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. This enables a more secure connection. Also if you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect. When you configure it 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 you have the Local ID set, the remote end of the tunnel must be configured to accept your Local ID. This menu item is available when *Topology* is *Dial up*.
Protected Subnet	Select the address or address group from the drop-down list and select the add icon to add the entry. You can add multiple entries.
Local Gateway	Type the local gateway IP address in the text field.

5. Click *OK* to save the settings.

Manage VPN gateways

You can manage VPN gateways from the *VPN Manager > IPsec VPN* pane. In the *All VPN Communities* list, select a community. Some options are available in the menu on the toolbar. Some options are available in the right-click menu. Right-click a VPN gateway to display the menu.

Option	Description
Create New	Create a new managed or external gateway.
Delete	Delete the selected gateway.
Edit	Edit the selected gateway.
Column Settings	In the *Column Settings* menu, select the column names that you want to display, and deselect the column names that you want to hide. Column settings include the option to restore columns to their default state.

SSL-VPN

You can use the *VPN Manager > SSL-VPN* pane to create and monitor Secure Sockets Layer (SSL) virtual private networks (VPN). You can also create and manage SSL VPN portal profiles.

Add SSL-VPN

To add SSL-VPN:

1. Go to *VPN Manager > SSL-VPN*.
2. Click *Add SSL VPN* or *Create New*. The *Create SSL VPN* pane is displayed.
3. Configure the following settings, and click *OK*.

Device	Select a FortiGate device or VDOM.
Connection Settings	Specify the connection settings.
Listen on Interface(s)	Define the interface which 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.
Source Address(es)	Specify one or more IPv4 IP addresses that FortiGate can assign to SSL VPN clients to use for the tunnel-mode session.

Source IPv6 Address(es)	Specify one or more IPv6 IP addresses that FortiGate can assign to SSL VPN clients to use for the tunnel-mode session.
Enable Idle Timeout	Select to enable idle timeout. In the *Timeout* box, type the period of time (in seconds) that the connection can remain inactive before the user must log in again. The range is from 10 to 28800 seconds. Setting the value to 0 will disable the idle connection timeout. This setting applies to the SSL VPN session. The interface does not time out when web application sessions or tunnels are up.
Server Certificate	Select the signed server certificate to use for authentication. Alternately, select a certificate template that is configured to use the FortiManager CA. See also Certificate templates on page 142.
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.
Port Precedence	Enable to give SSL-VPN higher priority than HTTPS, if both are enabled on the same port.
Encryption Key Algorithm	Select a cryptographic cipher suite.
Tunnel Mode Client Settings	Specify tunnel mode client settings. These settings determine how tunnel mode clients are assigned IP addresses.
Default IP Pool(s)	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.
Default IPv6 Pool(s)	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
Specify DNS/WINS Servers	Select to specify DNS/WINS servers. Enter up to two DNS servers (IPv4) to be provided for the use of clients.
Specify IPv6 DNS/WINS Servers	Select to specify DNS/WINS servers. Enter up to two DNS servers (IPv6) to be provided for the use of clients.
Authentication / Portal Mapping	Select the users and groups that can access the tunnel.

Default SSL-VPN portal profiles

The following pre-defined default portal profiles are available:

- Full-access
- Tunnel-access

- Web-access

Each portal type includes similar configuration options. You can also create custom portal profiles.

Create SSL-VPN portal profiles

To create portal profiles:

1. Go to *VPN Manager* > *SSL-VPN* > *Portal Profiles*.
2. Click *Create New*. The *New SSL-VPN Portal* pane is displayed.
3. Configure the following settings, and select *OK*.

Name	The name for the portal.
Enable 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 Routing Address, which is 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.
Enable 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 IPv6 Routing Address, which is 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.

Client Options	These options affect how the FortiClient application behaves when connected to the FortiGate VPN tunnel. When enabled, a check box for the corresponding option appears on the VPN login screen in FortiClient, and is not enabled by default. • Save Password - When enabled, if the user selects this option, their password is stored on the user's computer and will automatically populate each time they connect to the VPN. • Auto Connect - When enabled, if the user selects this option, when the FortiClient application is launched, for example after a reboot or system startup, FortiClient will automatically attempt to connect to the VPN tunnel. • Always Up (Keep Alive) - When enabled, if the user selects this option, 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	This is a text header that appears on the top of the web portal.
Theme	A color styling specifically for the web portal.
Page Layout	Select one column or two column layouts for the widgets that appear on the web portal page.
Include Status Information	Select to display the Status Information widget on the portal page. The Status Information widget displays the login name of the user, the amount of time the user has been logged in, and the inbound and outbound traffic statistics.
Include Connection Tool	Select to display the Connection Tool widget on the portal page. Use the Connection Tool widget to connect to a 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.
Include FortiClient Download	Select to include the FortiClient Download option in the web portal. This is enabled by default.
Prompt Mobile Users to Download FortiClient Application	If a remote user is using a web browser to connects to the SSL VPN in web mode, they are prompted to download the FortiClient application. The remote user can accept or reject the notification. If the user accepts, they are redirected to the FortiClient web site.
Include Login History	Select to include user login history on the web portal, and then specify the Number of History Entries.

Enable User Bookmarks	Select to 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 appears with the web page. Telnet, VNC, and RDP require a browser plugin. FTP and Samba replace the bookmarks page with an HTML file-browser.
Pre-Defined Bookmarks	Click the *Create* button to add a bookmark.
Limit Users to One SSL-VPN Connection at a Time	You can set the SSL VPN tunnel such that each user can only log into the tunnel one time concurrently per user per login. That is, once logged into the portal, they cannot go to another system and log in with the same credentials again. This option is disabled by default.
Advanced Options	Specify any number of advanced options. For a description of the options, see the *FortiOS Handbook*.

Monitor SSL-VPN

To monitor SSL-VPN:

1. Go to *VPN Manager* > *SSL-VPN*.
2. In the tree menu, click *Monitor*.

Manage SSL-VPN

You can manage SSL-VPN from the *VPN Manager* > *SSL-VPN* pane. Some options are available in the menu on the toolbar. Some options are available in the right-click menu. Right-click an SSL-VPN to display the menu.

Option	Description
Add SSL VPN	Create a new SSL-VPN.
Install Wizard	Launch the Install Wizard to install SSL-VPN settings to devices.
Create New	Create a new SSL-VPN.
Edit	Edit the selected SSL-VPN.
Delete	Delete the selected SSL-VPN.

Manage SSL-VPN portal profiles

You can manage SSL-VPN portal profiles from the *VPN Manager* > *SSL-VPN* > *Portal Profiles* pane. Some options are available in the menu on the toolbar. Some options are available in the right-click menu. Right-click a portal profile to display the menu.

Option	Description
Create New	Create a new portal profile.
Delete	Delete the selected portal profile.
Edit	Edit the selected portal profile.
Where Used	Display where the selected portal profile is used.
Select All	Select all portal profiles in the content pane.

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, 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 you defined in 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 address 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, which 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.

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.

For more information on IPsec VPN, see the *IPsec VPN for FortiOS* chapter of the *FortiOS Handbook available* from the Fortinet Document Library. See Managing policies on page 201 for information on creating a VPN policy on your FortiManager.

AP Manager

Use *AP Manager* to centrally manage FortiAP 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 a map.
WiFi templates	View, create, edit, and import AP profiles, SSIDs, and WIDS profiles.

Overview

The AP Manager pane allows you to manage, configure, and assign profiles to FortiAP devices. You can configure multiple profiles that can be assigned to multiple devices. Profiles are installed to devices when you install configurations to the devices.

The following steps provide an overview of using centralized AP management to configure and install profiles:

1. Create AP profiles.
   See WiFi templates on page 275.
2. Assign profiles to FortiAP devices.
   See Assigning profiles to FortiAP devices on page 268.
3. Install FortiAP profiles to devices.
   On the *Device Manager* pane, select the FortiGate device that controls the FortiAP device, then select *Install* > *Install Config* from the toolbar, and follow the prompts in the wizard. See Install wizard on page 116.

Managed APs

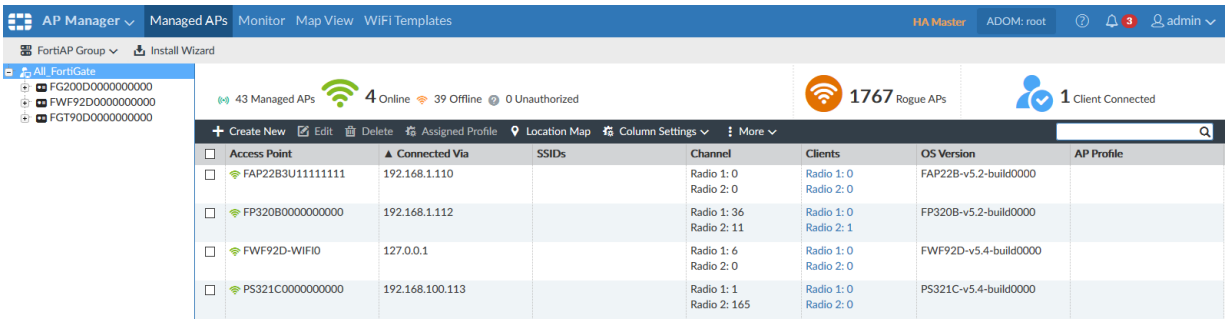
The *Managed APs* pane allows you to manage FortiAP devices that are controlled by FortiGate devices that are managed by the FortiManager.

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.

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 56.

Go to *AP Manager* > *Managed APs* to manage FortiAP devices. Managed APs are organized by their FortiGate controller and group.



Quick status bar

You can quickly view the status of devices on the *Managed AP* pane by using the quick status bar, which contains the following options:

- Managed APs
- Online
- Offline
- Unauthorized
- Rogue APs
- Client Connected

You can click each quick status to display in the content pane, or in a pop-up window, only the devices referenced in the quick status.

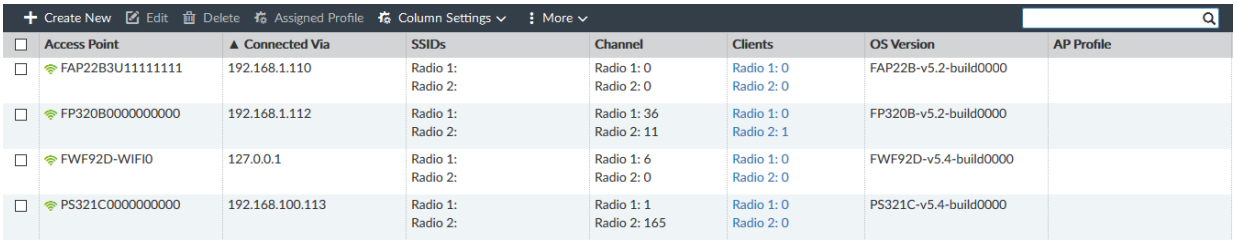
To view the quick status bar:

1. Ensure that you are in the correct ADOM.
2. Go to *AP Manager* > *Managed APs*. The quick status bar is displayed above the content pane.

3. In the tree menu, select a FortiGate, group, or *All_FortiGate*. 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.
5. Click *Rogue APs* to open the rogue AP list in a pop-up window.
6. 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.



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 268.
Column Settings	Adjust the columns visible on the content pane. This option is only available in the toolbar.
Authorize	Authorize an unregistered AP. See Authorizing and deauthorizing FortiAP devices on page 268. This option is also available in the toolbar by selecting *More*.
Deauthorize	Deauthorize a registered AP. See Authorizing and deauthorizing FortiAP devices on page 268. This option is also available in the toolbar by selecting *More*.
Grouping	Move the selected FortiAP devices into a new group. The APs must be the same model to be grouped. See FortiAP groups on page 267. This option is only available in the right-click menu.
Upgrade	Upgrade the AP. The AP must already be authorized.
Restart	Restart the AP. This option is only available in the toolbar, by selecting *More*.
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 271.

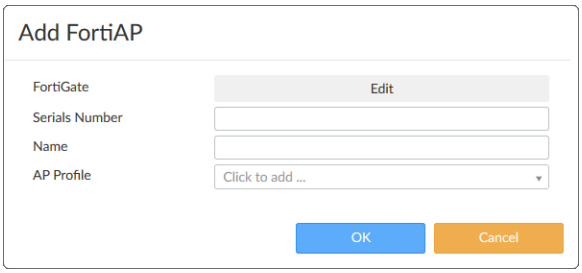
View Rogue APs	View the Rogue APs. See Rogue APs on page 269. This option is only available in the toolbar, by selecting *More*.
Search	Enter a search string into the search field to search the AP list. This option is only available in the toolbar.

The following information is available in the content pane:

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 271.
OS Version	The OS version on the FortiAP.
AP Profile	The AP Profile assigned to the device, if any.
FortiGate	The FortiGate unit that is managing the AP. Displayed only for unauthorized APs.
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.



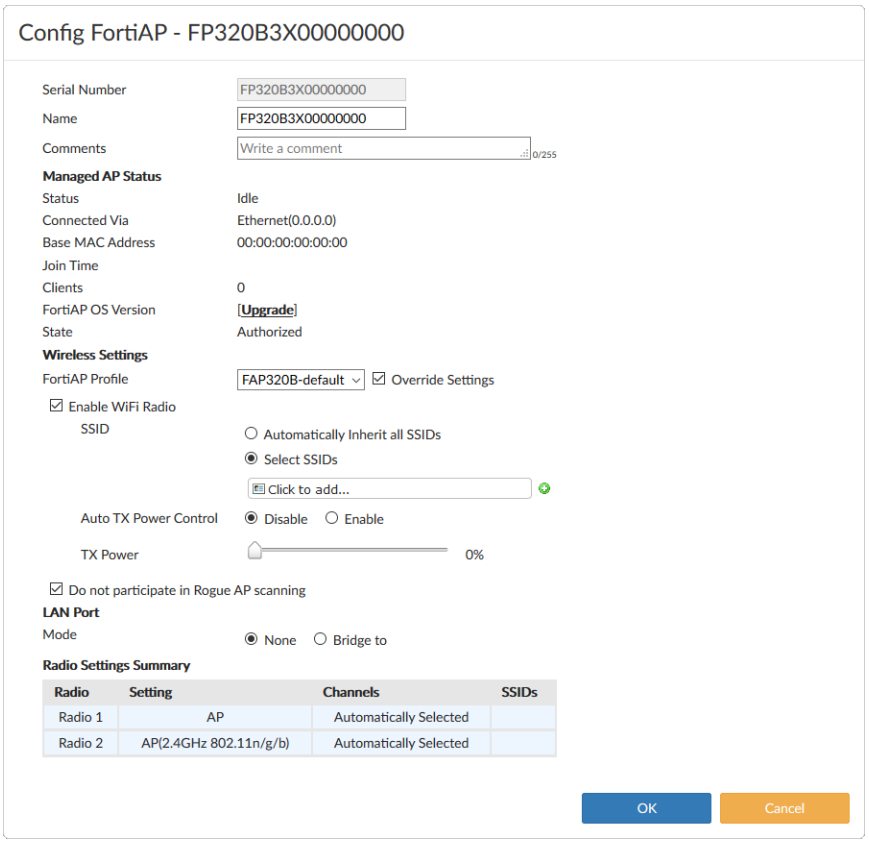
2. Enter the following information:

FortiGate	Select the FortiGate that the AP will be added to from the drop-down 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 drop-down list. See AP profiles on page 275.

3. Click *OK* to add the device.

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.



4. Edit the following options:

Serial Number	The device's serial number. This field cannot be edited.
Name	The name of the AP.
Comments	Comments about the AP, such as its location or function.
Managed AP Status	Various information about the AP.
Status	The status of the AP, such as *Connected*, or *Idle*.
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.
FortiAP OS Version	The AP's current firmware version. Select *Upgrade* to upgrade the firmware to a newer version if you have one available. See Firmware Management on page 134
State	The state of the AP, such as *Authorized*, or *Discovered*.

Wireless Settings	Assign a profile or configure radio settings manually.
FortiAP Profile	Select a profile from the drop-down list (see AP profiles on page 275), or select *Override Settings* to customize the WiFi radio settings for the AP (SSIDs, TX Power, and Rogue AP Scanning).
Do not participate in Rogue AP scanning	Select this option to not participate in scanning for rogues APs.
Radio Settings Summary	A table showing the current setting, channels, and SSIDs configured for the AP's radio or radios.

5. Click *Apply* to apply your changes.

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 it a firewall profile has been assigned to it.

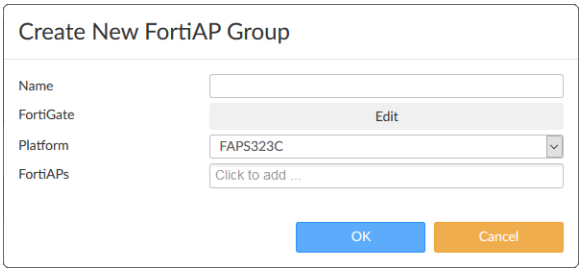
FortiAP groups

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.

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 275.

To assign profiles to 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 *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 drop-down list, then click *OK* to assign the profile.

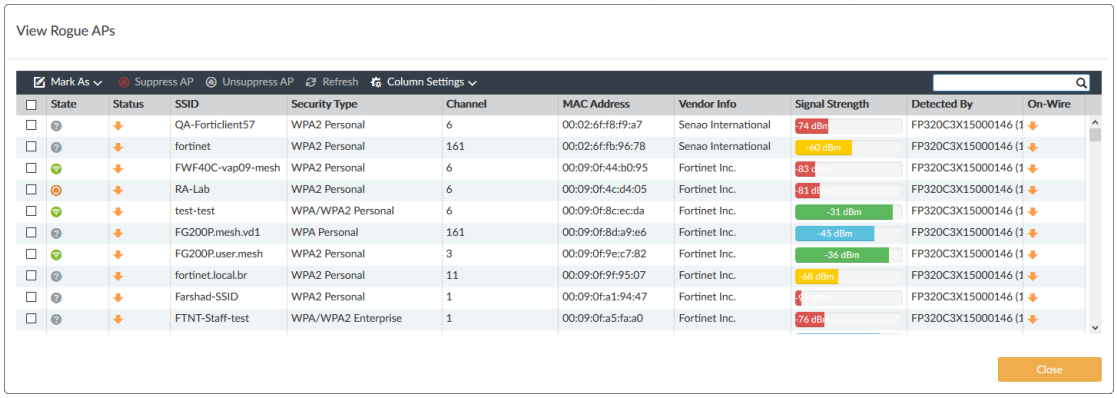
To install FortiAP profiles to devices:

1. Go to the *Device Manager* pane.
2. Select the FortiGate device that controls the FortiAP device, and from the *Install* menu, select *Install Config*.
3. Follow the prompts in the wizard. See Install wizard on page 116.

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.



The following options are available:

Mark As	Mark a rogue AP as: • *Accepted*: for APs that are an authorized part of your network or are neighboring APs that are not a security threat. • *Rogue*: for unauthorized APs that On-wire status indicates are attached to your wired networks. • *Unclassified*: the initial status of a discovered AP. You can change an AP back to unclassified if you have mistakenly marked it as *Rogue* or *Accepted*.

Suppress AP	Suppress the selected APs. This will prevent users from connecting to the AP. When suppression is activated against an AP, the controller sends deauthentication messages to the rogue AP's clients posing as the rogue AP, and also sends deauthentication messages to the rogue AP posing as its clients. Before enabling this feature, verify that operation of Rogue Suppression is compliant with the applicable laws and regulations of your region.
Unsurpress AP	Turn of suppression for the selected rogue APs.
Refresh	Refresh the rogue AP list.
Column Settings	Adjust the columns that are visible in the list.

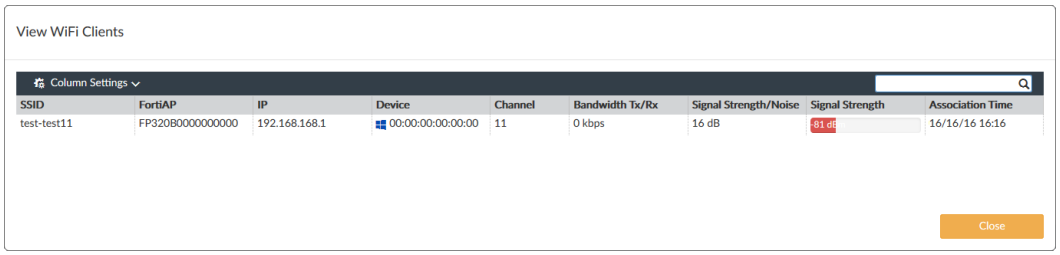
The following columns are available :

State	The state of the AP: • Suppressed: red suppressed icon • Rogue: orange rogue icon • Accepted: green wireless signal mark • Unclassified: gray question mark
Status	Whether the AP is active (green) or inactive (orange).
SSID	The wireless service set identifier (SSID) or network name for the wireless interface.
Security Type	The type of security currently being used.
Channel	The wireless radio channel that the access point uses.
MAC Adddess	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.

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*.



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.
Auth	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.

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.

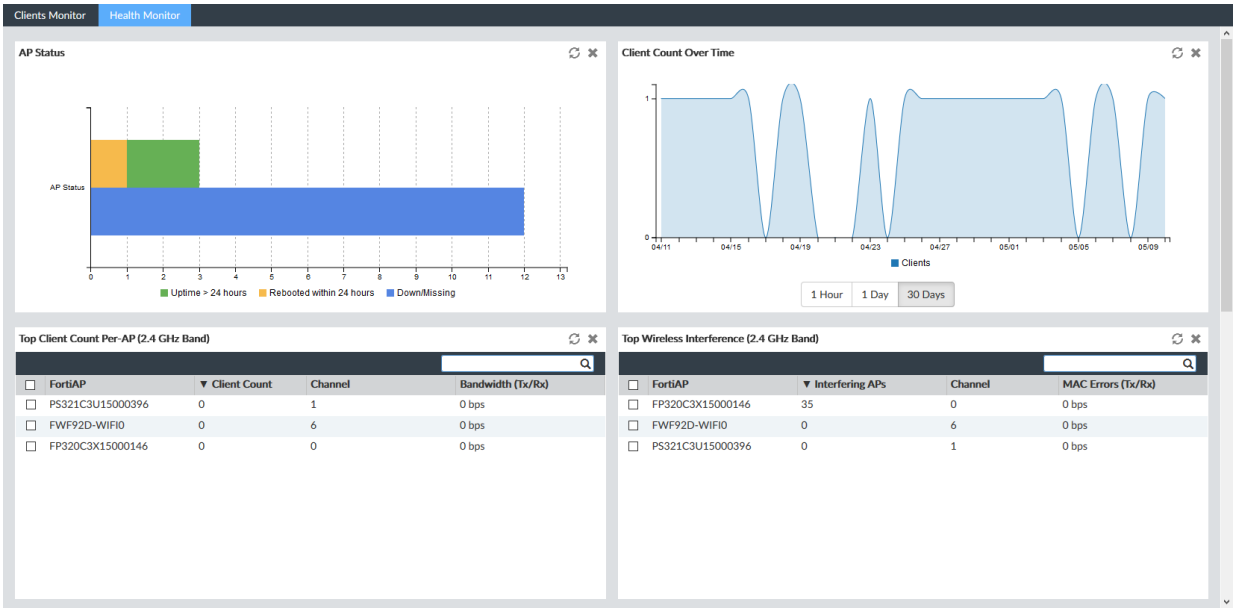
You can search the table by entering a search term in the search field in the toolbar. The visible columns can be adjusted by selecting *Column Settings* in the toolbar. The following columns are available:

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.
Assication Time	How long the client has been connected to this access point.
Auth	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	
Idle Time	The amount of time that the client has been idle.
Manufacturer	The manufacturer of the client device.
Rate	
Name	

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.



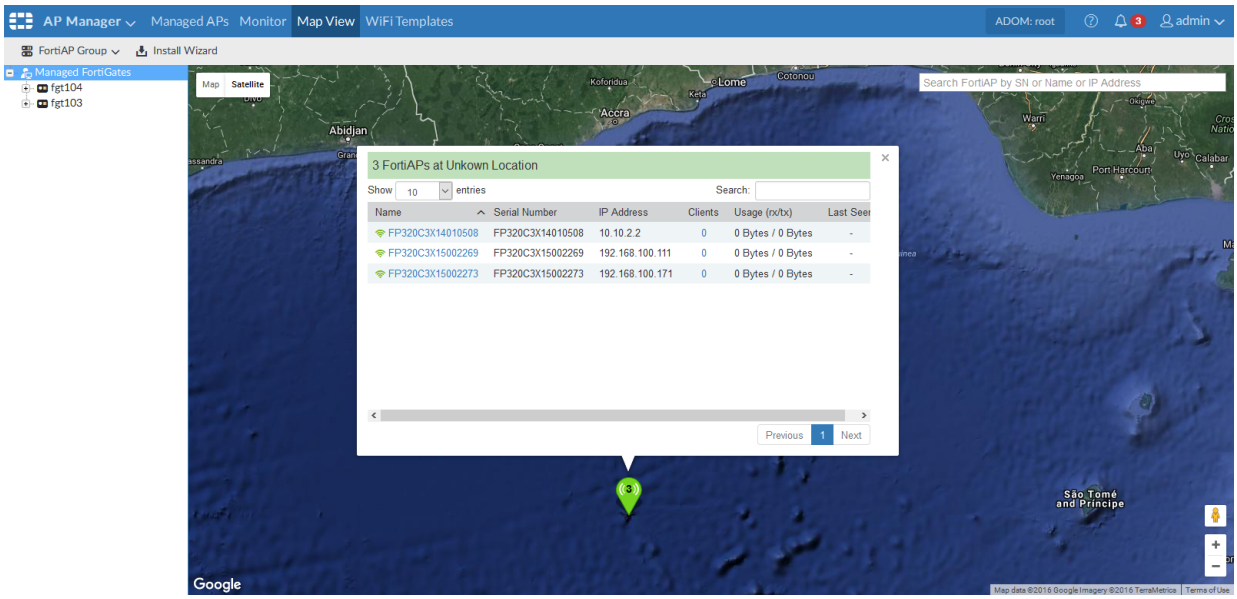
Widgets can be moved by clicking and dragging their title bar into different locations on the screen. The information in the widgets can be refreshed by clicking the refresh icon in the widget title bar. Widgets with tables can be sorted by any column by clicking the column name.

The following widgets are shown:

Widget	Description
AP Status	Displays a bar graph of: • *Uptime > 24 hours*: The number of APs that have been up for over 24 hours. • *Rebooted within 24 hours*: the number of APs that have been rebooted within the past 24 hours. • *Down/Missing*: Down or missing APs. Select a specific column to view a table of the APs represented in that column, along with other relevant information, such as the APs' IP address, and the time of its last reboot. Select the name of a column in the legend to add or remove it from the graph. This widget is only available when the *All FortiAPs* group is selected in the tree menu.
Client Count Over Time	A graph of the number of connected clients over the specified time period: 1 hour, 1 day, or 30 days. This widget is only available when the *All FortiAPs* group is selected in the tree menu.
Top Client Count Per-AP (2.4 GHz or 5 GHz Band)	Lists the number of clients in the 2.4GHz and 5GHz band for each FortiAP. Also includes columns for the channel and bandwidth of the AP.
Top Wireless Interference (2.4 GHz or 5 GHz Band)	Lists the number of interfering APs in the 2.4GHz and 5GHz band for each FortiAP. Also includes columns for the channel and the number of MAC Errors for each AP.
Login Failures Information	Lists the time of a log in failure, the SSID involved, the Host Name/MAC, and the User Name.

Map View

The Map View pane shows all of the FortiGate controllers on an interactive world map (Google Maps). 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 271). 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 263).

WiFi templates

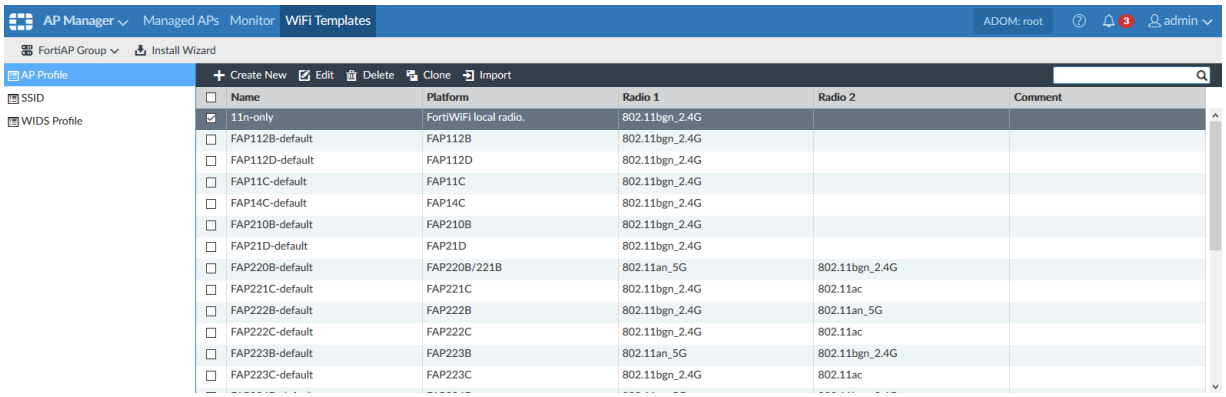
The *WiFi Templates* pane allows you to create and manage AP profiles, SSIDs, and Wireless Intrusion Detection System (WIDS) profiles that can be assigned to managed FortiAP devices.

Settings may vary for different ADOM versions.

AP profiles

AP profiles define radio settings for FortiAP models. The profile specifies details such as the operating mode of the device, SSIDs, and transmit power. Custom AP profiles can be created as needed for new devices.

To view AP profiles, ensure that you are in the correct ADOM, go to *AP Manager* > *WiFi Templates*, and select *AP Profile* in the tree menu.

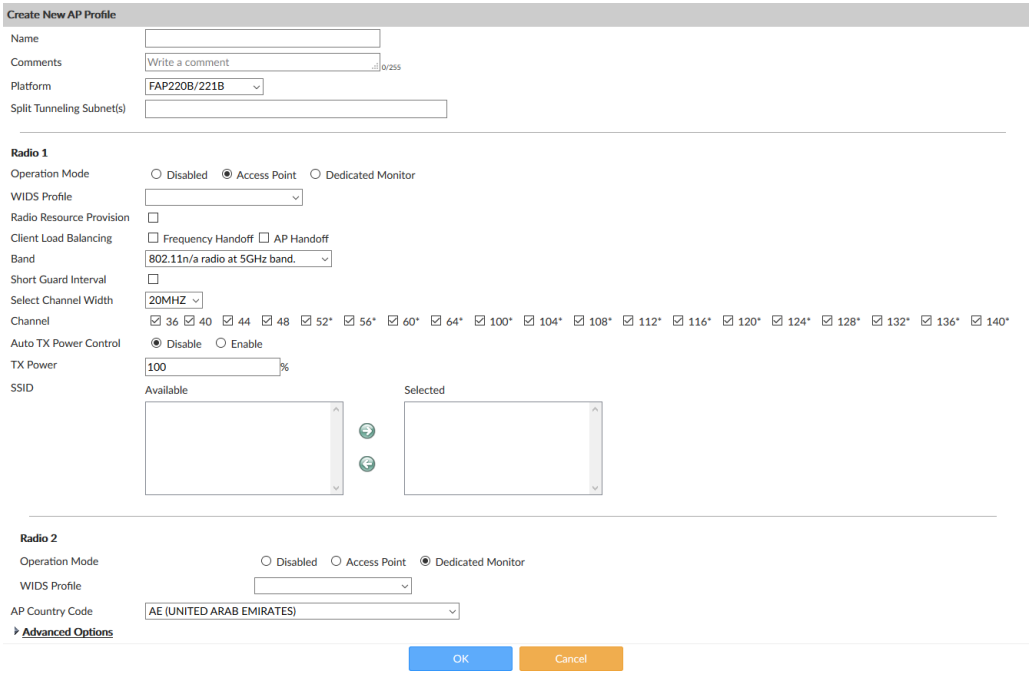


The following options are available in the toolbar and right-click menu:

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.



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 drop-down list.
Split Tunneling Subnet(s)	Enter the split tunneling subnet(s).
Radio 1 & 2	Configure the radio settings. The Radio 2 settings will only appear if the selected platform has two radios.
Operation Mode	Select the radio operation mode: • *Disabled*: The radio is disabled. No further radio settings are available. • *Access Point*: The device is an access point. • *Dedicated Monitor*: The device is a dedicated monitor. Only the *WIDS Profile* settings is available.
WIDS Profile	Select a WIDS profile from the drop-down list. See WIDS profiles on page 285.
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: *Frequency Handoff* and/or *AP Handoff*.
Band	Select the wireless protocol from the drop-down list. The available bands depend on the selected platform. In two radio devices, both radios cannot play in the same band.
Short Guard Interval	Select to enable the short guard interval. This option is only available for 2.4GHz 802.11n/g/b, and 5GHz 802.11n bands.
Select Channel Width	Select 20MHz or 40MHz channel width. This option is only available for 5GHz 802.11n bands.
Channel	Select the channel or channels to include. The available channels depend on the selected platform and band.
Auto TX Power Control	Optionally, enable automatic adjustment of transmit power, then specify the minimum and maximum power levels, dBm.
TX Power	If *Auto TX Power Control* is disabled, enter the TX power in the form of the percentage of the total available power.
SSID	Choose the SSIDs that APs using this profile will carry.
AP Country Code	Select the AP country code from the drop-down list.

Advanced Options	Configure advanced options for the SSID. • *allowaccess*: Allow management access to the managed AP via *http* and/or *telnet*. • *dtsl-in-kernal*: Enable/disable data channel DTLS in kernel. • *dtls-policy*: Select the WTP data channel DTLS policy: *clear-text* and/or *dtls-enabled*. • *handoff-roaming*: Enable/disable handoff when a client is roaming. • *handoff-rssi*: Etner 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-state*: Enable/disable use of LEDs on WTP. • *lldp*: Enable/disable LLDP. • *login-passwd*: Enter the log in password of the managed AP. • *login-passwd-change*: Select whether or not to allow the log in password to be changed, or to reset to the factory default setting. • *max-clients*: Enter the maximum number of STAs supported by the WTP. • *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*: Enable or disable the use of the WAN port as a LAN port.

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 drop-down list. The list will include all of the devices in the current ADOM.
3. Select the profile or profiles to be imported from the drop-down list.
4. Click *OK* to import the profile or profiles.

SSIDs

To view SSIDs, ensure that you are in the correct ADOM, go to *AP Manager* > *WiFi Templates*, and select *SSID* in the tree menu.

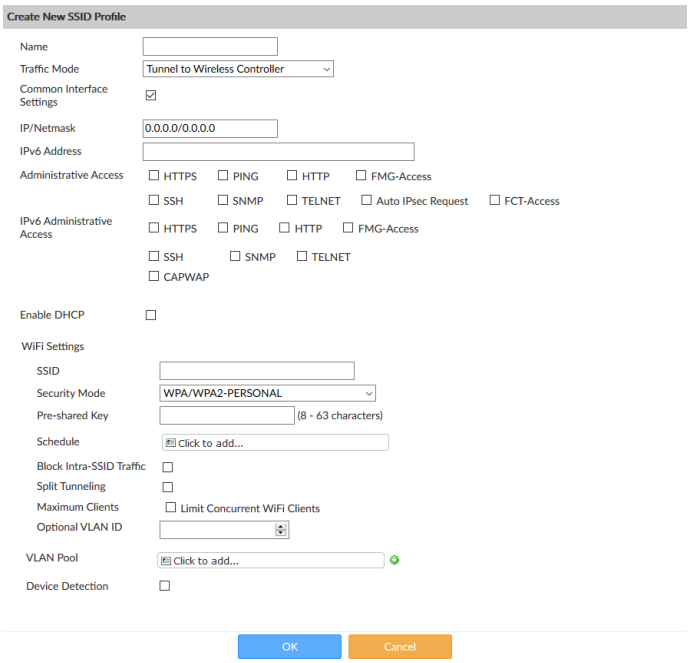
The following options are available in the toolbar and right-click menu:

Create New	Create a new SSID.
Edit	Edit the selected SSID.
Delete	Delete the selected SSID.
Clone	Clone the selected SSID.
Import	Import SSIDs from a connected FortiGate (toolbar only).

When creating a new SSID, the available options will change depending on the selected traffic mode: *Tunnel to Wireless Controller*, *Local bridge with FortiAP's Interface*, or *Mesh Downlink*.

To create a new SSID (Tunnel to Wireless Controller):

1. On the SSID pane, click *Create New* in the toolbar, or select it from the right-click menu. The *Create New SSID Profile* windows opens.



2. Enter the following information:

Name	Type a name for the SSID.
Traffic Mode	Select *Tunnel to Wireless Controller* from the drop-down list.
Common Interface Settings	Select to enable common interface settings.
IP/Netmask	Type the IP address and netmask.
IPv6 Address	Type the IPv6 address.
Administrative Access	Select the allowed administrative service protocols from: *HTTPS*, *HTTP*, *PING*, *FMG-Access*, *SSH*, *SNMP*, *TELNET*, *Auto IPsec Request*, and *FCT-Access*.
IPv6 Administrative Access	Select the allowed IPv6 administrative service protocols from: *HTTPS*, *HTTP*, *PING*, *FMG-Access*, *SSH*, *SNMP*, *TELNET*, and *CAPWAP*.
Enable DHCP	Select to enable and configure DHCP. Note: If *Mode* is *Relay*, only the *DHCP Server IP* and *Type* settings are available.
Address Range	Enter the DHCP address range.
Netmask	Enter the netmask.
Default Gateway	Select *Same As Interface IP* if the default gateway is the same as the interface IP, or select *Specify* and type a new gateway IP address.

DNS Server	Select *Same As System DNS* if the DNS server is the same as the system DNS, or select *Specify* and type a DNS server address.
Mode	Select *Server* or *Relay*.
DHCP Server IP	Enter the DHCP server IP address. This option is only available if *Mode* is set to *Relay*.
MAC Address Access Control List	The MAC address control list allows you to view the MAC addresses and their actions. It includes a default entry for unknown MAC addresses. • Click *Create New* to create a new IP MAC binding. • Select an address then click *Edit* to edit the MAC address. • Select an address or addresses then click *Delete* to delete the selected items. The unknown MAC address cannot be deleted.
Type	Select *Regular* or *IPsec*.
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	Select a security mode. The options are: *WPA/WPA2-PERSONAL* *WPA2-ONLY-PERSONAL* *WPA/WPA2-ENTERPRISE* *WPA2-ONLY-ENTERPRISE* *Captive Portal* *WPA/WPA2 Personal with Captive Portal* *OPEN* *WPA only Personal with Captive Portal* *WPA-ONLY-PERSONAL* *WPA2 Personal with Captive Portal* *WPA-ONLY-ENTERPRISE*
Pre-shared Key	Enter the pre-shared key for the SSID. This option is only available when the security mode includes WPA or WPA2 personal.
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 231.
Authentication	Select the authentication method for the SSID, either *Local* or *RADIUS Server*, then select the requisite server or group from the drop-down list. This option is only available when the security mode is includes WPA or WPA2 enterprise.

	Portal Type	Select the portal type, one of: *Authentication*, *Disclaimer + Authentication*, *Disclaimer Only*, or *Email Collection*. This option is only available when the security mode includes captive portal.
	Authentication Portal	Select *Local* or *External*. If *External* 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 drop-down list. Select the plus symbol to add multiple groups. This option is only available when the portal type includes authentication.
	Exempt List	Select the exempt list to add from the drop-down list. Select the plus symbol to add multiple lists. 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 or email collection.
	Redirect after Captive Portal	Select *Original Request* or *Specific URL*. If *Specific URL* is selected, enter the redirect URL. This option is only available when the security mode includes captive portal.
	Block Intra-SSID Traffic	Select to block intra-SSID traffic.
	Split Tunneling	Select to enable split tunneling.
	Maximum Clients	Select to limit the concurrent WiFi clients that can connect to the SSID. If selected, type the desired maximum number of clients.
	Optional VLAN ID	Select the VLAN ID in the text field using the arrow keys. Select 0 if VLANs are not used.
VLAN Pool		Select AP groups to add to the VLAN pool
Device Detection		Select to detect and identify devices connecting to the SSID.
	Add New Devices to Vulnerability Scan List	Select to add new devices to the vulnerability scan list.

3. Click *OK* to create the new tunnel to wireless controller SSID.

To create a new SSID (Local bridge with FortiAP's Interface):

1. On the SSID pane, click *Create New* in the toolbar.
2. Enter the following information:

Name	Type a name for the SSID.
Traffic Mode	Select *Local bridge with FortiAP's Interface* from the drop-down list.
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	Select a security mode. The options are: *WPA/WPA2-PERSONAL* *WPA/WPA2-ENTERPRISE* *OPEN* *WPA-ONLY-PERSONAL* *WPA-ONLY-ENTERPRISE* *WPA2-ONLY-PERSONAL* *WPA2-ONLY-ENTERPRISE*
Pre-shared Key	Enter the pre-shared key for the SSID. This option is only available when the security mode includes WPA or WPA2 personal.
Authentication	Select the authentication method for the SSID, either *Local* or *RADIUS Server*, then select the requisite server or group from the drop-down list. This option is only available when the security mode is includes WPA or WPA2 enterprise.
Maximum Clients	Select to limit the concurrent WiFi clients that can connect to the SSID. If selected, type the desired maximum number of clients. Type 0 for no limit.
Optional VLAN ID	Select the VLAN ID in the text field using the arrow keys. Select 0 if VLANs are not used.
VLAN Pool	Select AP groups to add to the VLAN pool
Device Detection	Select to detect and identify devices connecting to the SSID.
Add New Devices to Vulnerability Scan List	Select to add new devices to the vulnerability scan list.

3. Click *OK* to create the new local bridge SSID.

To create a SSID (Mesh Downlink):

1. On the SSID pane, click *Create New* in the toolbar.
2. Enter the following information:

Name	Type a name for the SSID.
Traffic Mode	Select *Mesh Downlink* from the drop-down list. T
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	Select a security mode. The options are: *WPA/WPA2-PERSONAL* *WPA-ONLY-PERSONAL* *OPEN* *WPA2-ONLY-PERSONAL*
Pre-shared Key	Enter the pre-shared key for the SSID.
Maximum Clients	Select to limit the concurrent WiFi clients that can connect to the SSID. If selected, type the desired maximum number of clients. Type 0 for no limit.
VLAN Pool	Select AP groups to add to the VLAN pool
Device Detection	Select to detect and identify devices connecting to the SSID.
Add New Devices to Vulnerability Scan List	Select to add new devices to the vulnerability scan list.

3. Click *OK* to create the SSID.

To edit an SSID:

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* 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 an SSID or SSIDs:

1. Select the SSID or SSIDs 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 SSID or SSIDs.

To clone an SSID:

1. Either select an SSID and click *Clone* in the toolbar, or right-click on the SSID name, and select *Clone*. The *Clone SSID* dialog box opens.
2. Edit the settings as required. The 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 drop-down 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* drop-down list.
4. Click *OK* to import the SSID or SSIDs.

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.

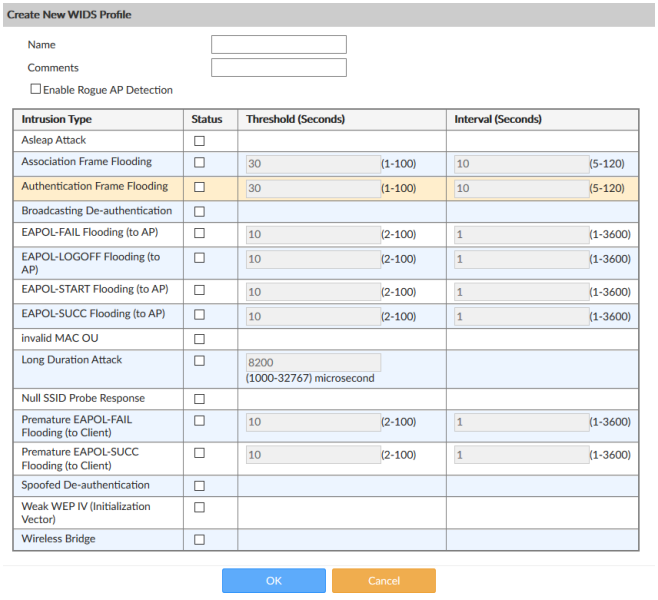
To view WIDS profiles, ensure that you are in the correct ADOM, go to *AP Manager* > *WiFi Templates*, and select *WIDS Profile* in the tree menu.

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.



2. Enter the following information:

Name	Enter a name for the profile.
Comments	Optionally, enter comments.
Enable Rogue AP Detection	Select to enable rogue AP detection.
Background Scan Every Second(s)	Enter the number of seconds between background scans.
Disable Background Scan During Specified Time	Select to disables background scanning during the specified time. Specify the days of week, and the start and end times.
Enable Passive Scan Mode	Select to enable passive scan mode.
Enable On-Wire Rogue AP Detection	Select to enable on-wire rogue AP detection. When enabled you can select to auto suppress rogue APs in foreground scan.
Intrusion Type	The intrusion types that can be detected.
Status	Select to enable the intrusion type.
Threshold	If applicable, enter a threshold for reporting the intrusion, in seconds except where specified.
Interval (sec)	If applicable, enter the interval for reporting the intrusion, in seconds.

3. Click *OK* to create the new WIDS profile.

Intrusion types

Intrusion Type	Description
Asleap 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 De-authentication	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.

Intrusion Type	Description
EAPOL Packet Flooding (to AP)	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the AP with these packets can be a denial of service attack. Several types of EAPOL packets can be detected: • EAPOL-FAIL • EAPOL-LOGOFF • EAPOL-START • EAPOL-SUCC
Invalid MAC OU	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 8200.
Null SSID Probe Response	When a wireless client sends out a probe request, the attacker sends a response with a null SSID. This causes many wireless cards and devices to stop responding.
Premature EAPOL Packet Flooding (to client)	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the client with these packets can be a denial of service attack. Two types of EAPOL packets can be detected: • EAPOL-FAIL • EAPOL-SUCC
Spoofed De-authentication	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 drop-down list. The list will include all of the devices in the current ADOM.
3. Select the profile or profiles to be imported from the drop-down list.
4. Click *OK* to import the profile or profiles.

FortiClient Manager

The *FortiClient Manager* pane enables you to centrally manage FortiClient profiles for multiple FortiGate devices and monitor FortiClient endpoints that are connected to FortiGate devices.

Endpoint control ensures that workstation computers (endpoints) and other network devices meet security requirements, otherwise they are not permitted access. Endpoint control enforces the use of FortiClient Endpoint Security and pushes a FortiClient profile to the FortiClient application.

For information about FortiClient, see the *FortiClient Administration Guide*.

Additional configuration options and shortcuts are available using the right-click menu. Right-click on different parts of the navigation panes in the GUI to access these menus.

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

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.

Overview

Centralized FortiClient management is enabled by default. You use the *FortiClient Manager* pane to enable FortiTelemetry and FortiClient enforcement on FortiGate interfaces as well as create and assign FortiClient profile packages to one or more FortiGate devices or VDOMs. Profile packages are installed to devices when you install configurations to the devices.

The following steps provide an overview of using centralized FortiClient management to configure, assign, and install FortiClient profiles:

To create and assign FortiClient profile packages:

1. Create a FortiClient profile package. Creating FortiClient profile packages on page 297.
2. Select the profile package, and create one or more FortiClient profiles. See Creating FortiClient profiles on page 298.
3. Enable FortiTelemetry on FortiGate interfaces. See Enabling FortiTelemetry on interfaces on page 292.
4. Enable FortiClient enforcement on FortiGate interfaces. See Enabling endpoint control on interfaces on page 292.

5. Assign profile packages to FortiGate interfaces. See Assigning FortiClient profile packages to devices on page 293.

To install configuration changes to devices:

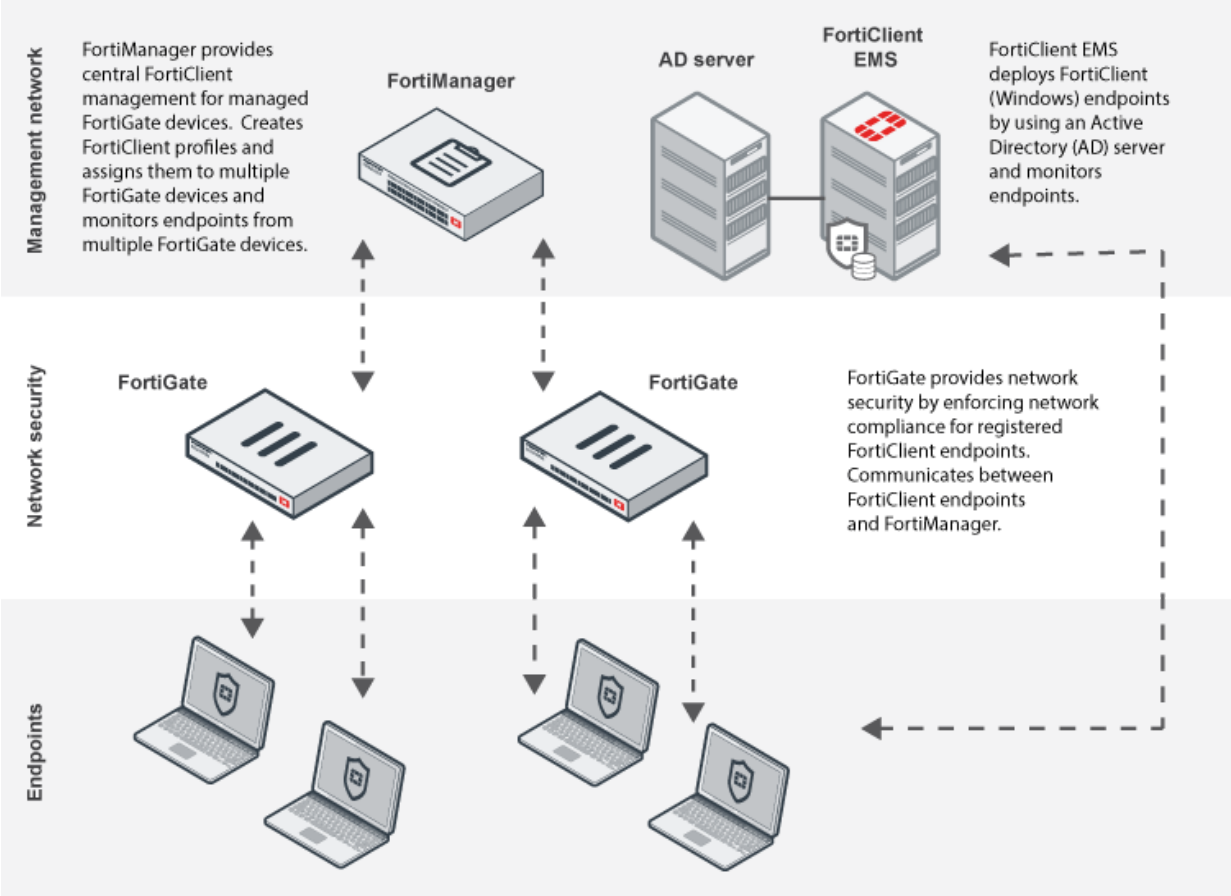
1. On the *FortiClient Manager > FortiClient Profiles* pane, click *Install Wizard*.
2. Follow the prompts in the wizard. See Install wizard on page 116.

You can also monitor FortiClient endpoints. See Monitor on page 293.

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 and use the profiles for deployment, or you can use FortiClient EMS to create profiles. When FortiClient endpoints connect FortiClient Telemetry to FortiGate or 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 115.

Viewing devices

The *FortiClient Manager* > *FortiTelemetry* pane displays FortiGate devices with central FortiClient management enabled.

To view devices:

1. Ensure 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. Ensure 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: • Block • Unblock • Quarantine • Release Quarantine • Unregister
Column Settings	Click to select which columns to display on the *Monitor* pane. Select *Reset to Default* to return to the default column settings.
By Interface	Click to organize the display of FortiClient endpoints by the undetected interfaces and interface name. In the *Device* column, click *Undetected* 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: *Noncompliant* and *Exempt*. In the *Device* column, click *Noncompliant* or *Exempt* 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.
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: • 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: • Compliant • Endpoint is not compliant with FortiClient profile • Quarantined • FortiTelemetry is disabled 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.

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 *Profile Package* 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 *Edit* to edit the profile. Alternatively, double click the profile to open the *Edit FortiClient Profile* pane.
Delete	Select a profile, and click *Delete* to delete the profile from the ed FortiClient profile package. Alternately, right-click a profile, and select *Delete*.
Import	Select to import a FortiClient profile from an existing device or VDOM into the selected FortiClient profile package.
Column Settings	In the *Column Settings* menu, select the column names that you want to display, and deselect the column names that you want to hide. Column settings include the option to restore columns to their default state.

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: *Warning*, *Block*, or *Auto-Update*.

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 consists of the following sections:

- Non-compliance action
- Compliance rules

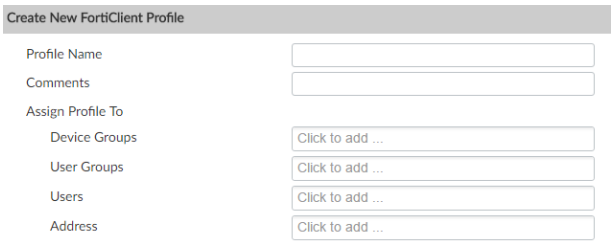
For more information on configuring FortiClient Profiles and Endpoint Control, see the *FortiOS Handbook* and the *FortiClient Administration Guide*.

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. Click *Create New*.
   The *Create New FortiClient Profile* pane opens.

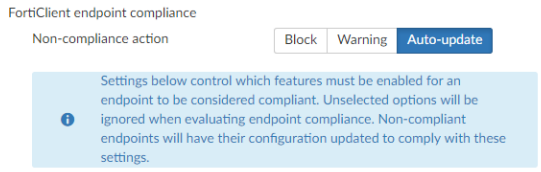


4. Enter the following information:

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.

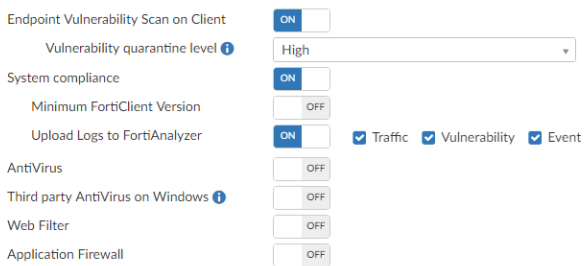
Assign Profile To	Identify where to assign the profile: • Device Groups: Select device groups in the drop-down list. • User Groups: Select user groups in the drop-down list. • Users: Select users in the drop-down list. • Address: Select addresses in the drop-down list. You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN.

5. Set the *Non-compliance action* for FortiClient endpoint compliance:



Block	Select *Block* to provide the compliance rules but no configuration information to FortiClient endpoints. When FortiClient endpoints fail to comply with the compliance rules, endpoint access to the network is blocked. Non-compliance information is displayed in the FortiClient console. The administrator or endpoint user is responsible for reading the noncompliance information and updating FortiClient software on the endpoints to adhere to the compliance rules.
Warning	Select *Warning* to provide the compliance rules but no configuration information to FortiClient endpoints. When FortiClient endpoints fail to comply with the compliance rules, endpoint users are warned, but allowed to continue accessing the network. Non-compliance information is displayed in the FortiClient console. The administrator or endpoint user is responsible for reading the noncompliance information and updating FortiClient software on the endpoints to adhere to the compliance rules.
Auto-update	Select *Auto-update* to provide the compliance rules and configuration information from FortiGate. The configuration information provided by FortiGate helps FortiClient endpoints remain compliant. Non-compliance information is displayed in the FortiClient console. The FortiManager administrator and endpoint user are responsible for keeping endpoints compliant.

6. Set the compliance rules for FortiClient endpoints:



Endpoint Vulnerability Scan on Client		Toggle on or off. Toggle *ON* to include the setting in the compliance rules. Toggle *OFF* to exclude the setting from the compliance rules.
	Vulnerability quarantine level	When *Endpoint Vulnerability Scan on Client* is toggled to *ON*, you can select a quarantine level from the *Vulnerability quarantine level* list.
System compliance		Toggle on or off. Toggle *ON* to include the setting in the compliance rules and display additional options, such as minimum FortiClient version. Toggle *OFF* to exclude the setting from the compliance rules.
	Minimum FortiClient Version	When *System compliance* is toggled *ON*, you can enable or disable *Minimum FortiClient Version*. Toggle *ON* to display the *Windows endpoints* and *Mac endpoints* options.
	Windows endpoints	When *Minimum FortiClient Version* is toggled *ON*, you can type the minimum version of FortiClient that is required on endpoints running Windows operating systems.
	Mac endpoints	When *Minimum FortiClient Version* is toggled *ON*, you can type the minimum version of FortiClient that is required on endpoints running Macintosh operating systems.
	Upload logs to FortiAnalyzer	When *System compliance* is toggled *ON*, you can enable or disable the uploading of FortiClient logs from endpoints to FortiAnalyzer. Toggle *ON* to enable uploading of logs to FortiAnalyzer, and then select the types of logs to upload. You can upload *Traffic*, *Vulnerability*, and/or *Event* logs.
AntiVirus		Toggle on or off. Toggle *ON* to include AntiVirus in the compliance rules and display additional options, such as *Realtime Protection*. Toggle *OFF* to exclude the setting from the compliance rules.
	Realtime Protection	When *AntiVirus* is toggled *ON*, you can enable or disable *Realtime Protection*. Toggle *ON* to enable Realtime Protection and display additional options, such as *Up-to-date signatures*.
	Up-to-date signatures	When *AntiVirus* and *Realtime Protection* are toggled *ON*, you can enable or disable *Up-to-date signatures*. Toggle *ON* to enable up-to-date signatures.
	Scan with FortiSandbox	When *AntiVirus* and *Realtime Protection* are toggled *ON*, you can enable or disable scanning with FortiSandbox. Toggle *ON* to enable scanning with FortiSandbox.
Third party AntiVirus on Windows		Toggle on or off. Toggle *ON* to include a requirement of third-party AntiVirus software on the endpoint in the compliance rules.
Web Filter		Toggle on or off. Toggle *ON* to include *Web Filter* in the compliance rules. Toggle *OFF* to exclude the setting from the compliance rules.

	Profile	When *Web Filter* is toggled *ON*, you can select a web filter profile. A default profile is selected by default.
Application Firewall		Toggle on or off. Toggle *ON* to include *Application Firewall* in the compliance rules. Toggle *OFF* to exclude the setting from the compliance rules.
	Application Control Sensor	When *Application Firewall* is toggled *ON*, you can select an application control sensor. A default application control sensor is selected by default.

7. 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

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 drop-down 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.

FortiGuard

The FortiGuard Distribution Network (FDN) provides FortiGuard services for your FortiManager system and its managed devices and FortiClient agents. The FDN is a world-wide network of FortiGuard Distribution Servers (FDS), which update the FortiGuard services on your FortiManager system on a regular basis so that your FortiManager system is protected against the latest threats.

The FortiGuard services available on the FortiManager system include:

- Antivirus and IPS engines and signatures
- Web filtering and email filtering rating databases and lookups (select systems)
- Vulnerability scan and management support for FortiAnalyzer

To view and configure these services, go to *FortiGuard* > *Advanced 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 unregistered devices, add your devices to the device list, or change the option to allow service to unregistered devices. For more information, see the *FortiManager CLI Reference*.

  For information about FDN service connection attempt handling or adding devices, see Device Manager on page 94.
- Enable and configure the FortiManager system's built-in FDS. For more information, see Configuring the network on page 40.
- 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 307.
- 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 95.

This section contains the following topics:

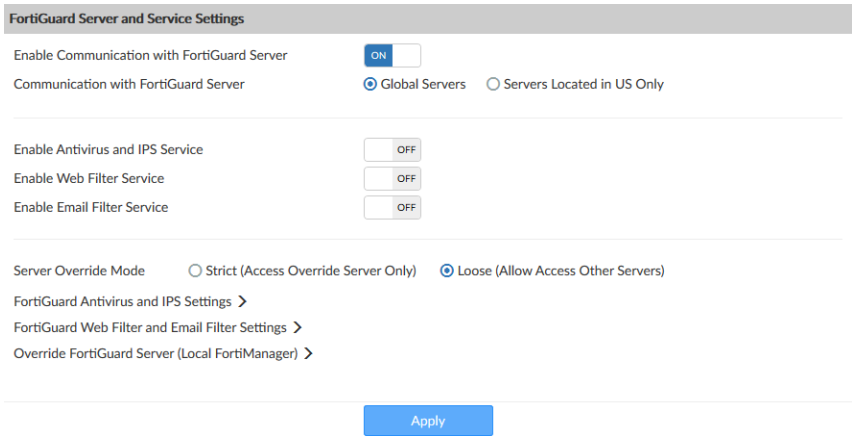
For information on current security threats, virus and spam sample submission, and FortiGuard service updates available through the FDN, including antivirus, IPS, web filtering, and email filtering, see the FortiGuard Center website, http://www.-fortiguard.com/.

Settings

FortiGuard > *Settings* provides a central location for configuring and enabling your FortiManager system's built-in FDS as an FDN override server.

By default, this option is enabled. After configuring FortiGuard and configuring your devices to use the FortiManager system as their FortiGuard server, you can view overall and per device statistics on FortiGuard service benefits.

To operate in a closed network, disable communication with the FortiGuard server. See Operating as an FDS in a closed network on page 308.



Enable communication with FortiGuard servers.	When toggled *OFF*, you must manually upload packages, databases, and licenses to your FortiManager. See Operating as an FDS in a closed network on page 308.

Communication with FortiGuard Server	Select *Servers Located in the US Only* to limit communication to FortiGuard servers located in the USA. Select *Global Servers* to communicate with servers anywhere.
Enable Antivirus and IPS Service	Toggle *ON* to enable antivirus and intrusion protection service. When on, select what versions *FortiGate*, *FortiClient*, *FortiAnalyzer*, and *FortiMail* to download updates for.
Enable Web Filter and 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.
Server Override Mode	Select *Strict (Access Override Server Only)* or *Loose (Allow Access Other Servers)* override mode.
FortiGuard Antivirus and IPS Settings	Configure antivirus and IPS settings. See FortiGuard antivirus and IPS settings on page 305.
FortiGuard Web Filter and Email Filter Settings	Configure web and email filter settings. See FortiGuard web and email filter settings on page 306
Override FortiGuard Server (Local FortiManager)	Configure web and email filter settings. See Override FortiGuard server (Local FortiManager) on page 307

FortiGuard antivirus and IPS settings

In this section you can enable settings for FortiGuard Antivirus and IPS settings.

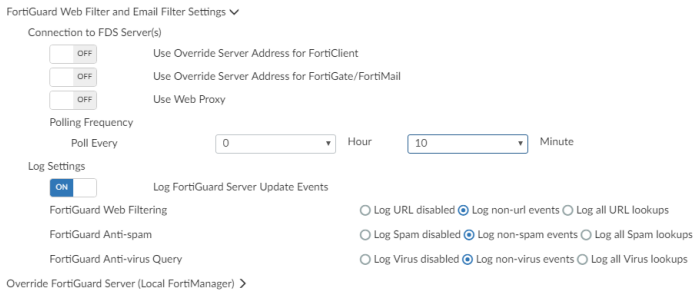
Configure the following settings:

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. Click the add icon to add additional override servers. Click the delete icon to remove entries. To override the default server for updating FortiGate/FortiMail devices' FortiGuard services, see Overriding default IP addresses and ports on page 314.
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 312.
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 313.

Scheduled Regular Updates	Configure when packages are updated without manually initiating an update request. To schedule regular service updates, see Scheduling updates on page 314.
Update	Select to immediately update the configured antivirus and email filter settings.
Advanced	Enables logging of service updates and entries. If either option is not enabled, you will not be able to view these entries and events when you select *View FDS and FortiGuard Download History*.

FortiGuard web and email filter settings

In this section you can enable settings for FortiGuard Web Filter and Email Filter.



Configure the following settings:

Connection to FDS server (s)	Configure connections for overriding the default built-in FDS or web proxy server for web filter and email filter settings. To override an FDS server for web filter and email filter services, see Overriding default IP addresses and ports on page 314. To enable web filter and email filter service updates using a web proxy server, see Enabling updates through a web proxy on page 313.
Use Override Server Address for FortiClient	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries.
Use Override Server Address for FortiGate/FortiMail	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries. To override the default server for updating FortiGate device's FortiGuard services, see Overriding default IP addresses and ports on page 314.
Use Web Proxy	Configure the FortiManager system's built-in FDS to connect to the FDN through a web proxy. IPv4 and IPv6 are supported. To enable updates using a web proxy, see Enabling updates through a web proxy on page 313.
Polling Frequency	Configure how often polling is done.

Log Settings	Configure logging of FortiGuard web filtering, email filter, and antivirus query events. • *Log FortiGuard Server Update Events*: enable or disable • *FortiGuard Web Filtering*: Choose from *Log URL disabled*, *Log non-url events*, and *Log all URL lookups*. • *FortiGuard Anti-spam*: Choose from *Log Spam disabled*, *Log non-spam events*, and *Log all Spam lookups*. • *FortiGuard Anti-virus Query*: Choose from *Log Virus disabled*, *Log non-virus events*, and *Log all Virus lookups*. To configure logging of FortiGuard web filtering and email filtering events, see Logging FortiGuard web or email filter events on page 316

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.

Configure the following settings:

Additional number of Private FortiGuard Servers (Excluding This One)	Select the add icon to add a private FortiGuard server. Select the delete icon to remove entries. When adding a private server, you must type its IP address and time zone.
Enable Antivirus and IPS Update Service for Private Server	When one or more private FortiGuard servers are configured, update anti-virus and IPS through this private server instead of using the default FDN. This option is available only when a private server has been configured.
Enable Web Filter and Email Filter Update Service for Private Server	When one or more private FortiGuard servers are configured, update the web filter and email filter through this private server instead of using the default FDN. This option is available only when a private server has been configured.
Allow FortiGates to Access Public FortiGuard Servers When Private Servers Unavailable	When one or more private FortiGuard servers are configured, managed FortiGate units will go to those private servers for FortiGuard updates. Enable this feature to allow those FortiGate units to then try to access the public FDN servers if the private servers are unreachable. This option is available only when a private server has been configured.

The FortiManager system's network interface settings can restrict which network interfaces provide FDN services. For more information, see Configuring the network on page 40.

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* > *Advanced 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 312.
3. Click *Apply*.
   The built-in FDS attempts to connect to the FDN.

See also the *FortiOS HandBook: FortiGuard Licensing for FortiGates with Limited or No Connectivity* document in the Document Library at http://docs.fortinet.com/fortigate/admin-guides.

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 the network on page 40.
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. For additional FDN troubleshooting information, including FDN server selection, see FDN port numbers and protocols on page 314.

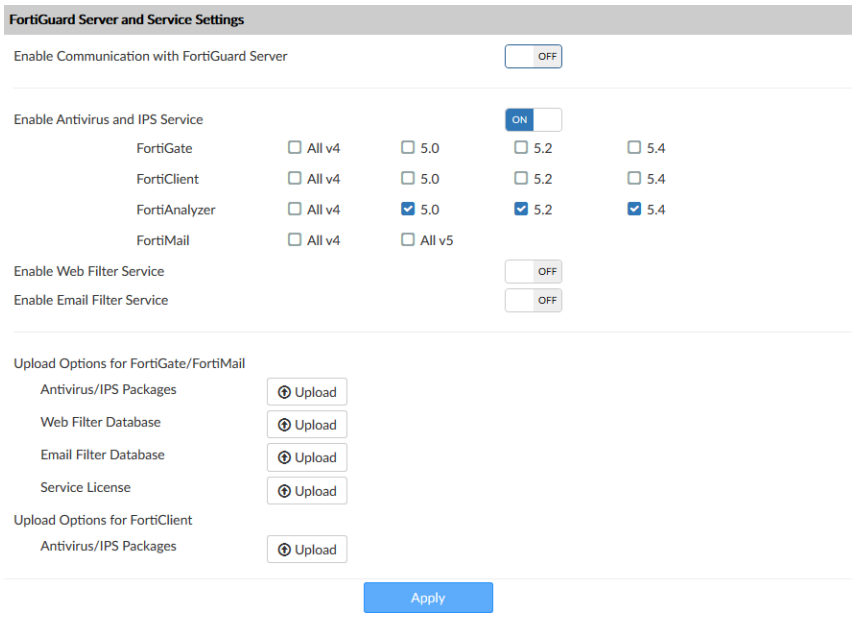
Operating as an FDS in a closed network

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.

Go to *FortiGuard* > *Settings* to configure FortiManager as a local FDS server and to upload update packages and license.



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 *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. Select *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. Select *OK* to upload the package to FortiManager. As the database can be large, uploading with the CLI is recommended. See the instructions below.

Email Filter Database	Select to upload the email filter database. Browse for the file you downloaded from the Customer Service & Support portal on your management computer. Select *OK* to upload the package to FortiManager. As the database can be large, uploading with the CLI is recommended. See the instructions below.
Service License	Select to import the FortiGate license. Browse for the file on your management computer. Select *OK* to upload the package to FortiManager. A license file can be obtained from support by requesting your account entitlement for the device.
Upload Options for FortiClient	
AntiVirus/IPS Packages	Select to upload the FortiClient AntiVirus/IPS packages. Browse for the file you downloaded from the Customer Service & Support portal on your management computer. Select *OK* to upload the package to FortiManager.

Uploading packages with the CLI

Packages and licenses can be uploaded using the CLI. This should be used when the packages being uploaded are large, like database packages.

To upload packages and license files using the CLI:

1. If not already done, disable communications with the FortiGuard server and enable a closed network with the following CLI commands:
```
config fmupdate publicnetwoek
   set status disable
end
```
2. Upload an update package or license:
   a. Load the package or license file to an FTP, SCP, or TFTP server
   b. Run the following CLI command:
```
execute fmupdate { ftp | scp | tftp } import < av-ips | fct-av | url | spam |
    file-query | license-fgt | license-fct | custom-url | domp > <remote_file>
    <ip> <port> <remote_path> <user> <password>
```

Configuring devices to use the built-in FDS

After enabling and configuring the FortiManager system's built-in FDS, you can configure devices to use the built-in FDS by providing the FortiManager system's IP address and configured port as their override server.

Devices are not required to be registered with FortiManager system's *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. If the settings are disabled, see Network on page 40.

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 unregistered devices

The built-in FDS replies to FortiGuard update and query connections from devices registered with the device manager's device list. If the FortiManager is configured to allow connections from unregistered devices, unregistered 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 unregistered 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* pane. For information on widget settings, see Customizing the dashboard on page 327.
2. Click inside the console to connect.
3. To configure the system to add unregistered 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 unregistered 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*.

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

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 313.

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 inter-mediary 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* > *Advanced Settings*.
2. Click the arrow to expand *FortiGuard Antivirus and IPS Settings*; see FortiGuard antivirus and IPS settings on page 305.
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 av-ips 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* > *Advanced 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 > Advanced Settings*.
2. If you want 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 enter the IP address and/or port number for all FortiGate units.
3. If you want 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*.
4. Toggle *ON* beside *Use Override Server Address for FortiGate/FortiMail* and/or *Use Override Server Address for FortiClient* and type 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 307.

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 on a very frequent basis. By configuring a scheduled update, you are guaranteed to have a relatively 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 > Advanced Settings*.
2. Click the arrow to expand *FortiGuard Antivirus and IPS Settings*; see FortiGuard antivirus and IPS settings on page 305.

3. Toggle *ON* beside *Schedule Regular Updates*.
4. Specify an hourly, daily, or weekly schedule.
5. Click *Apply*.

To schedule Web Filtering and Email Filter polling:

1. Go to *FortiGuard* > *Advanced Settings*.
2. Click the arrow to expand *FortiGuard Web Filter and Email Filter Settings*.
3. In *Polling Frequency*, select the number of hours and minutes of the polling interval.
4. Click *Apply*.

If you have formatted your FortiManager system's hard disk, polling and lookups will fail until you restore the URL and email filter databases. For more information, see Restoring the URL or antispam database on page 317.

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* > *Advanced 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) (0)*. 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 registered FortiGate devices which use the FortiManager system's FDS.

To log updates and histories to the built-in FDS:

1. Go to *FortiGuard* > *Advanced Settings*.
2. Click the arrow to expand *FortiGuard Antivirus and IPS Settings*; see FortiGuard antivirus and IPS settings on page 305.
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* > *Advanced 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 registered 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* > *Advanced Settings*.
2. Click the arrow to expand *FortiGuard Web Filtering and Email Filter Settings*.
3. Select the log settings:

Log FortiGuard Server Update Events	Enable or disable logging of FortiGuard server update events.
FortiGuard Web Filtering	
Log URL disabled	Disable URL logging.
Log non-URL events	Logs only non-URL events.

Log all URL lookups	Logs all URL lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
FortiGuard Anti-spam	
Log Spam disabled	Disable spam logging.
Log non-spam events	Logs email rated as non-spam.
Log all Spam lookups	Logs all spam lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
FortiGuard Anti-virus Query	
Log Virus disabled	Disable virus logging.
Log non-virus events	Logs only non-virus events.
Log all Virus lookups	Logs all virus queries sent to the FortiManager system's built-in FDS by FortiGate devices.

4. Click *Apply*.

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.
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.
Object Type	The type of object for the package.
Package Received	The name of the package.
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 *Change* 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 drop-down 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

The *Service Status* page shows a list of all the managed FortiGate devices, their last update time, and their status. A device's status can be one of the following:

- Up to Date: The latest package has been received by the FortiGate unit.
- Never Updated: The FortiGate unit has never requested or received the package.
- Pending: The FortiGate unit has an older version of the package due to an acceptable reason (such as the scheduled update time having not come yet).
- Problem: The FortiGate unit missed the scheduled query, or did not correctly receive the latest package.
- Unknown: The FortiGate unit's status is not currently known.

Pending updates can also be pushed to the devices, either individually or all at the same time. The list can be refreshed by selecting *Refresh* in the toolbar.

This page displays the following:

Push Pending	Select the device or devices in the list, then click *Push Pending* in the toolbar to push pending updates to the device or devices.

Push All Pending	Select *Push All Pending* in the toolbar to push pending updates to all of the devices in the list.
Refresh	Select to refresh the list.
Device	The device serial number or host name is displayed.
Status	The service update status. Hover the mouse cursor over a pending icon to view the package to be installed.
Last Update Time	The date and time of the last update.

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

The view the received packages, go to *FortiGuard* > *Query Server Management* > *Receive Status*.

The following information is displayed:

Refresh	Select to refresh 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.

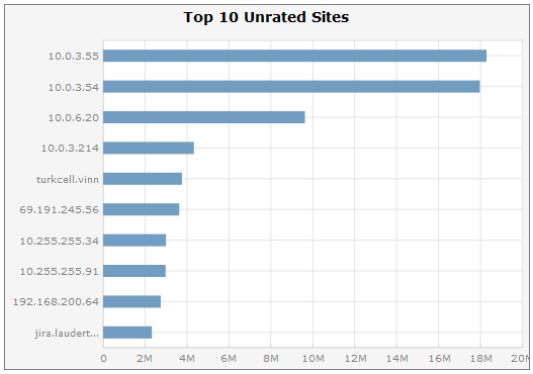
It shows the update times, the events that occurred, the statuses of the updates, and the versions downloaded.

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., and FortiExtender.

You can download only those images that are needed from the FDS systems, and customize which firmware images are available for deployment.

The following information and settings are available:

Import Images	Select to open the firmware image import list.
Models	From the drop-down list, select *All* to show all the available models on the FortiGuard server, or select *Managed* to show only the models that are currently being managed by the FortiManager device.
Product	Select a managed product type from the drop-down list.
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. Select *Change* to open the *Change Version* dialog box, then select the desired version from the drop-down list and select *OK* to change the preferred version.
Size	The size of the firmware image.
Status	The status of the image, that is, from where it is available.
Action Status	The status of the current action being taken.
Release Notes	A link to a copy of the release for the firmware image that has been downloaded.
Download/Delete	Download the firmware image from the FDS if it is available. If the firmware images has already been downloaded, then delete the firmware image from the FortiManager device.

For information about upgrading your FortiManager device, see the FortiManager Release Notes or contact Fortinet Customer Service & Support.

To import a firmware image:

1. Go to *FortiGuard* > *Firmware Images*, and click *Import Images* in the toolbar.
2. Select a device in the list, and click *Import* in the toolbar.
3. In the *Upload Firmware Image* dialog box, click *Browse* to browse to the desired firmware image file.
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.

FortiAnalyzer Features

When FortiAnalyzer features are enabled for the FortiManager unit, the following panes are available:

FortiView	View summaries of log data. For example, you can view top threats to your network, top sources of network traffic, top destinations of network traffic and so on.
Log View	View log messages from managed devices. You can view the traffic log, event log, or security log information.
Event Monitor	View events from logs that you want to monitor. You can specify what log messages to display as events by configuring event handlers.
Reports	Generate reports of data from logs.

On the System Settings pane, the following options are also available:

- You can configure log storage settings on the *System Settings* > *Advanced* > *Device Log Settings* pane.
- You can also view information about log storage on the *System Settings* > *Storage Info* pane.
- You can set up fetcher management on the *System Settings* > *Fetcher Management* pane.

You use the FortiAnalyzer feature to view and analyze logs from devices managed by the FortiManager unit. In addition to enabling FortiAnalyzer features, the managed devices must be configured to forward logs to the FortiManager device.

For information about using FortiAnalyzer features, see the *FortiAnalyzer Administration Guide* or the FortiAnalyzer Online Help.

Enabling FortiAnalyzer features

To enable FortiAnalyzer features:

1. Go to *System Settings* > *Dashboard*.
2. Set the *FortiAnalyzer Features* toggle switch to *On*.

Configuring log settings for managed devices

In addition to enabling FortiAnalyzer features on the FortiManager device, you must also configure the managed devices to send logs to the FortiManager device.

The FortiManager unit will receive logs only from managed devices that are configured to send logs to the FortiManager unit. For information on configuring FortiGate devices to send logs to FortiManager units, see the FortiOS documentation for the device.

Viewing logs and reports

For information on using FortiAnalyzer features, see the *FortiAnalyzer Administration Guide*.

To view logs and reports:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *FortiView*, *Log View*, *Event Monitor*, or *Reports*.

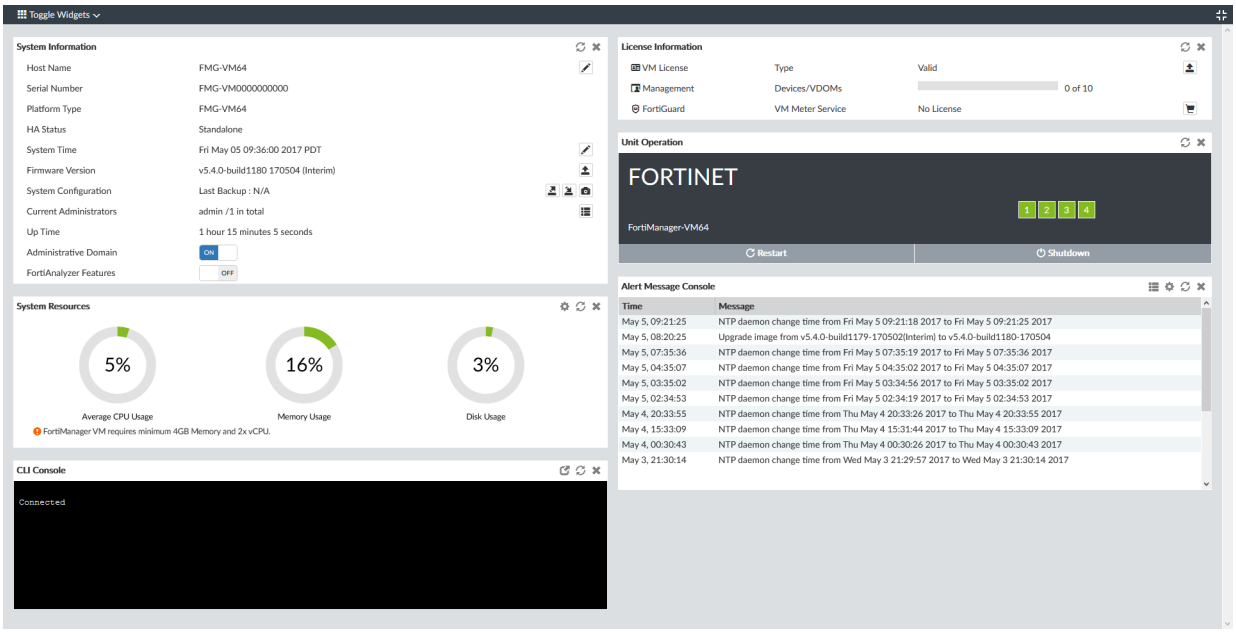
System Settings

System Settings allows you to manage system options for your FortiManager unit.

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.

Dashboard

The *Dashboard* contains widgets that provide performance and status information and enable you to configure basic system settings. The dashboard also contains a CLI widget that lets you use the command line through the GUI.



The following widgets are available:

Widget	Description
System Information	Displays basic information about the FortiManager system, such as up time and firmware version. You can also enable or disable Administrative Domains and FortiAnalyzer features. For more information, see System Information widget on page 327. From this widget you can manually update the FortiManager firmware to a different release. For more information, see Firmware images on page 321. The widget fields will vary based on how the FortiManager is configured, for example, if ADOMs are enabled.
System Resources	Displays the real-time and historical usage status of the CPU, memory and hard disk. For more information, see System Resources widget on page 334.
License Information	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 334. From this widget you can manually upload a license for FortiManager VM systems.
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 335.
CLI Console	Opens a terminal window that enables you to configure the FortiManager unit using CLI commands directly from the GUI. This widget is hidden by default. For more information, see CLI Console widget on page 335.
Alert Message Console	Displays log-based alert messages for both the FortiManager unit itself and connected devices. For more information, see Alert Messages Console widget on page 336.
Log Receive Monitor	Displays a real-time monitor of logs received. You can select to view data per device or per log type. For more information, see Log Receive Monitor widget on page 336. The *Log Receive Monitor* widget is available when *FortiAnalyzer Features* is enabled.
Insert Rate vs Receive Rate	Displays the log insert and receive rates. For more information, see Insert Rate vs Receive Rate widget on page 337. The *Insert Rate vs Receive Rate* widget is available when *FortiAnalyzer Features* is enabled.
Log Insert Lag Time	Displays the log insert lag time, in seconds. For more information, see Log Insert Lag Time widget on page 337. The *Log Insert Lag Time* widget is available when *FortiAnalyzer Features* is enabled.

Widget	Description
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 338. The *Disk I/O*widget is available when *FortiAnalyzer Features* 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 widgets	Select *Toggle Widgets* from the toolbar, then select the name widget you need to add.
Delete a widget	Click the *Close* icon in the widget's title bar.
Reset the dashboard	Select *Toggle Widgets* > *Reset to Default* from the toolbar. The dashboards will be reset to the default view.

System Information widget

The information displayed in the *System Information* widget is dependent on the FortiManager models 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 329.
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 *FMG-VM* (virtual machine).
HA Status	Displays if FortiManager unit is in High Availability mode and whether it is the Master or Slave unit in the HA cluster. For more information see High Availability on page 339.

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 329.
Firmware Version	The version number and build number of the firmware installed on the FortiManager unit. To update the firmware, you must download the latest version from the Customer Service & Support website at 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 330.
System Configuration	The date of the last system configuration backup. The following actions are available: • Click the backup button to backup the system configuration to a file; see Backing up the system on page 331. • Click the restore to restore the configuration from a backup file; see Restoring the configuration on page 332. You can also migrate the configuration to a different FortiManager model by using the CLI. See Migrating the configuration on page 332. • Click the check point to revert the system to a prior saved configuration; see Creating a system checkpoint on page 333.
Current Administrators	The number of administrators that are currently logged in. Click the current session list button to view the session details for all currently logged in administrators. See for more information.
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 52.
Log Storage Policy	Available when ADOMs are disabled and FortiAnalyzer features are enabled. Specifies how much FortiManager disk space to use for log storage, how long to keep logs indexed in the database to support analysis, and how long to keep compressed logs on disk before automatically deleting the logs. Select *[Change]* to configure.
Policy Package Version	Displays the policy package version.
VPN Management Mode	Available when ADOMs are disabled. Displays whether centralized VPN management is enabled. Click the *Change VPN Management Mode* icon to enable and disable. When enabled, you can use the *VPN Manager* tab for central management.

WAN Link Load Balance	Available when ADOMs are disabled. Displays whether centralized WAN link load balancing is enabled. Click the *Change WAN Link Load Balance Mode]* icon to enable and disable. When enabled, you can use the *Device Manager* > *WAN Link Load Balance* pane for central management.
FortiAnalyzer Features	Displays whether FortiAnalyzer features are enabled. Toggle the switch to change the FortiAnalyzer features state. *FortiAnalyzer Features* are not available on available on the FortiManager 100C.

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. For more information about the *System Information* widget.
- 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 check mark to change the host name.

Configuring the system time

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

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

To configure the date and time:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, click the edit system time button next to the *System Time* field.
3. Configure the following settings to either manually configure the system time, or to automatically synchronize the

FortiManager unit's clock with an NTP server:

System Time	The date and time according to the FortiManager unit's clock at the time that this pane was loaded or when you last clicked the *Refresh* button.
Time Zone	Select the time zone in which the FortiManager unit is located and whether or not the system automatically adjusts for daylight savings time.
Update Time By	Select *Set time* to manually set the time, or *Synchronize with NTP Server* to automatically synchronize the time.
Set Time	Manually set the data and time.
Select Date	Set the date from the calendar or by manually entering it in the format: YYYY/MM/DD.
Select Time	Select the time.
Synchronize with NTP Server	Automatically synchronize the date and time.
Sync Interval	Enter how often, in minutes, that 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.

4. Click the check mark to apply your changes.

Updating the system firmware

To take advantage of the latest features and fixes, FortiManager provides two ways to upgrade its firmware: manually or through the FDN.

For information about upgrading your FortiManager device, see the FortiManager Release Notes or contact Fortinet Customer Service & Support.

Back up the configuration and database before changing the firmware of your FortiManager unit. Changing the firmware to an older or incompatible version may reset the configuration and database to the default values for that firmware version, resulting in data loss. For information on backing up the configuration, see Backing up the system on page 331.

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

To manually update the FortiManager firmware:

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, click the update firmware button next to *Firmware Version*.
4. Select *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support website.
5. Select *OK* to upload the file.

   The time required to upload the firmware file varies by the size of the file and the speed of your network connection. When the file transfer is complete, a prompt appears:

   ```
   Manual upload release complete. It will take a few minutes to unpack the
   uploaded release. Please wait.
   ```

6. Wait until the unpacking process completes, then refresh the page. The firmware package file name will appear in the *Releases Available For Upgrade* section after you refresh the page.
7. Select the firmware package, then select the icon in the *Upgrade Firmware* column and select *OK* in the dialog box that appears. The FortiManager unit installs the firmware and restarts.

   If you changed the firmware to an earlier version whose configuration is not compatible, you may need to do first-time setup again. For instructions, see the *FortiManager QuickStart Guide* for your unit.
8. Update the vulnerability management engine and definitions.

Installing firmware replaces the current network vulnerability management engine with the version included with the firmware release that you are installing. After you install the new firmware, make sure that your vulnerability definitions are up-to-date. For more information, see FortiGuard on page 303.

The FortiManager firmware can also be updated through the FDN. For more information, see Firmware images on page 321.

Backing up the system

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

You can perform backups manually or at scheduled intervals. You can also create a backups - called checkpoints - that define a point where the FortiManager and network management is stable and functioning. Should any future configurations cause issues, you have a point where the system is stable.

Fortinet recommends backing up all configuration settings from your FortiManager unit before upgrading the FortiManager firmware.

To back up the FortiManager configuration:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, click the backup button next to *System Configuration*.
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 15 characters.

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

Restoring the configuration

You can use the following procedure to restore your FortiManager configuration from a backup file on your management computer. If your FortiManager unit is in HA mode, switch to Standalone mode.

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

To restore the FortiManager configuration:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, click the restore button next to *System Configuration*.
3. Configure the following settings then select *OK*.

Choose Backup File	Select *Browse* to find the configuration backup file you want to restore.
Password	Type the encryption password, if applicable.
Overwrite current IP, routing and HA settings	Select the check box to overwrite the current IP, routing and HA settings.
Restore in Offline Mode	Informational check box. 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.

You need the username and password for the FortiManager model to which you are migrating the configuration file.

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 331.
3. In the other FortiManager model, go to *System Settings* > *Dashboard*.
4. In the *CLI Console* widget, type the following command:

```
exec migrate all-settings < ftp | scp | sftp > <server> <filepath> <user> <password>
    [cryptpasswd]
```

Creating a system checkpoint

You can create a system checkpoint backup to capture a specific configuration. This backup provides a history where the FortiManager and FortiGate units are completely in sync. Should there be a major failure, you can completely revert the FortiManager to when it was in working order. These are, in essence, snapshots of your FortiManager managed network system.

You should make a system checkpoint backup before installing new firmware to devices or making a major configuration change to the network. If the update or modification causes problems, you can quickly revert to an earlier known “good” version of the configuration to restore operation.

A system checkpoint backup includes the system configuration of the FortiManager unit.

Please note the following:

- The system checkpoint does not include the FortiGate settings.
- For policy package specific settings, after reverting to a checkpoint, you need to re-install policy packages to update FortiGate policy and related configuration.
- For non-policy package settings, after reverting to a checkpoint, you must trigger FortiGate to auto-update and overwrite the checkpoint reverted configuration. Alternatively, you can disable the auto update function in System Settings and re-install the checkpoint reverted configuration to FortiGate.

To create a system checkpoint:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, click the check point button next to *System Configuration*. The *System Checkpoint List* opens.
3. Select *Create New*. The *Add New System Checkpoint* dialog box opens.
4. In the *Comments* box, type a description, up to 63 characters, for the reason or state of the backup.
5. Select *OK*. The system checkpoint task will be run and the checkpoint will be created.

To revert to a system checkpoint:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, click the check point button next to *System Configuration*. The *System Checkpoint* table opens.
3. Select the system checkpoint in the table then click *Revert*.
4. A confirmation dialog box will open. Select *OK* to continue.

When reverting to a system checkpoint, the FortiManager will reboot.

To delete a system checkpoint:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, click the check point button next to *System Configuration*. The *System Checkpoint* table opens.
3. Select the system checkpoint in the table then select the *Delete* in the toolbar.
4. A confirmation dialog box will open. Select *OK* to continue.

Enable or disable FortiAnalyzer features

The FortiAnalyzer feature set can enabled or disabled via the CLI using the following command:

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

You can also enable or disable these features in the FortiManager GUI. The FortiAnalyzer feature set includes: *FortiView*, *Event Management*, and *Reports*. Other menu items are FortiAnalyzer related including *Device Log Settings* and *File Management*.

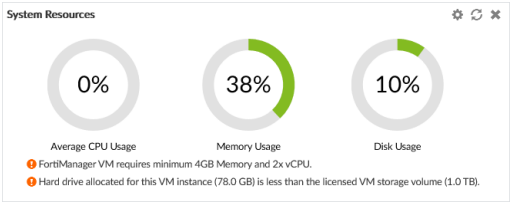
To enable or disable the FortiAnalyzer features, toggle the switch in the *FortiAnalyzer Features* field in the *System Information* widget on the *System Settings* dashboard. The FortiManager will reboot to apply the change.

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

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 will be displayed if the amount of memory or the number of CPU assigned are too low, or if the allocated hard drive space is less than the licensed amount. These warnings are also be shown in the notification list (see GUI overview on page 34). Clicking on a warning will open the *FortiManagerVM Install Guide*.

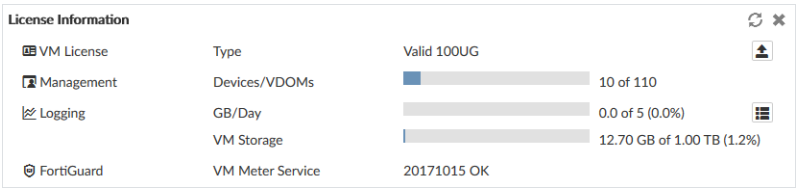


To toggle between real-time and historical data, click *Edit* in the widget toolbar, select *Historical* or *Real-time*, edit the other settings as required, then click *OK*.

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

License Information widget

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

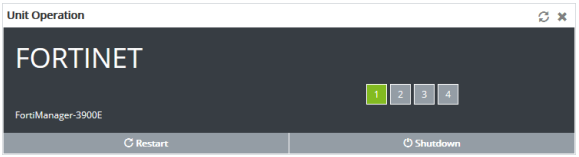


VM License	VM license information and status. click the upload license button to upload a new VM license file. This field is only visible for FortiManager VM.
Management	
Device/VDOMs	The total number of devices and VDOMs connected to the FortiManager and the total number of device and VDOM licenses.
Logging	This section is only shown when *FortiAnalyzer Features* is enabled. For more information, see FortiAnalyzer Features on page 323.
GB/Day	The gigabytes per day of logs allowed and used for this FortiManager. Click the show details button to view the GB per day of logs used for the previous 6 days.
VM Storage	The amount of VM storage used and remaining. This field is only visible for FortiManager VM.
FortiGuard	The FortiGuard license status. Click the purchase button to go to the Fortinet Customer Service & Support website, where you can purchase a license. This field is only visible for FortiManager VM.

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 that the port is connected. Grey indicates that 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.



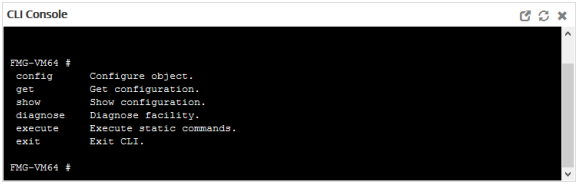
CLI Console widget

The *CLI Console* widget enables you to type command lines through the GUI, without making a separate Telnet, SSH, or local console connection to access the CLI.

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

For information on available CLI commands, see the *FortiManager CLI Reference*.

When using the *CLI Console* you are logged in under 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 in to or out of the console.



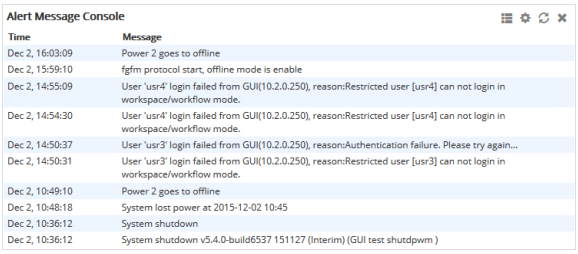
Click *Detach* in the widget toolbar to open the widget in a separate window.

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 that the event occurred.

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



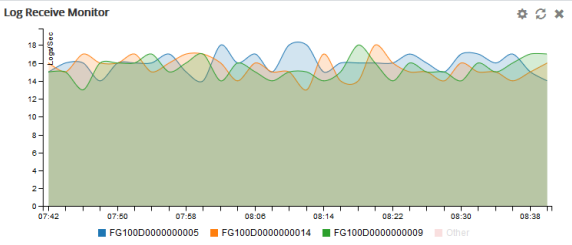
Click *Edit* from the widget toolbar to view the *Alert Message Console Settings*, where you can adjust the number of entries that are visible in the widget, and the refresh interval.

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

Log Receive Monitor widget

The *Log Receive Monitor* widget displays the rate at which the FortiManager unit receives logs over time. You can select to display log data by 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 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 enabled. For more information, see FortiAnalyzer Features on page 323.

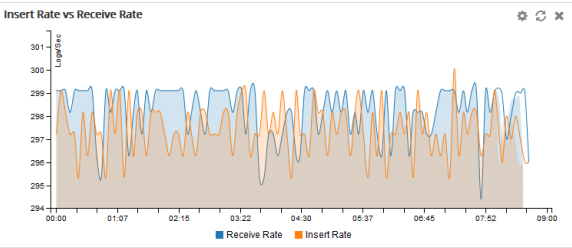
Insert Rate vs Receive Rate widget

The *Insert Rate vs Receive Rate* widget displays the log insert and log receive rates in a line graph.

- 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 that are 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 and a specific time. Click *Receive Rate* or *Insert Rate* to remove that data from the graph. Click the edit icon in the widget toolbar to adjust the time interval shown on the graph (last 1 hour, 8 hours, or 24 hours) and the refresh interval (60 - 240 seconds, 0 to disable) of the widget.

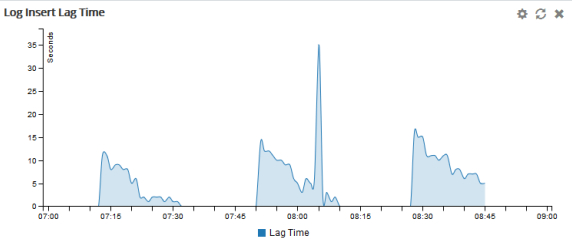


This widget is only available when the FortiAnalyzer features are enabled. For more information, see FortiAnalyzer Features on page 323.

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 (last 1 hour, 8 hours, or 24 hours) and the refresh interval (60 - 240 seconds, 0 to disable) of the widget.

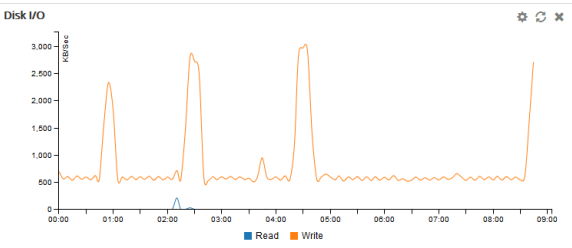


This widget is only available when the FortiAnalyzer features are enabled. For more information, see FortiAnalyzer Features on page 323.

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 (last 1 hour, 8 hours, or 24 hours), and the refresh interval (5 - 240 seconds, 0 to disable) of the chart.

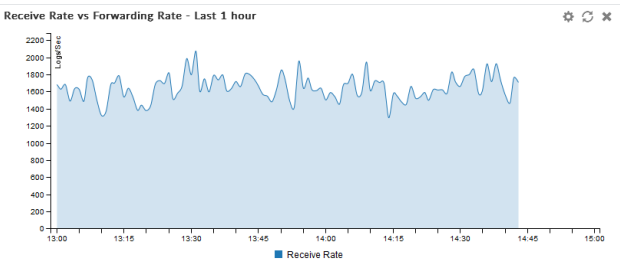


This widget is only available when the FortiAnalyzer features are enabled. For more information, see FortiAnalyzer Features on page 323.

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 enabled. For more information, see FortiAnalyzer Features on page 323.

Storage info

The *Storage Info* pane is available when FortiAnalyzer features are enabled. On the *Storage Info* pane, you can configure the amount of FortiManager disk space that is used for log storage. After you configure log storage capacity, you can monitor storage statistics. For details, see the *FortiAnalyzer Administration Guide*, available in the Fortinet Document Library.

High Availability

This section provides a general description of FortiManager High Availability (HA). This section also describes all HA configuration options and includes some basic HA configuration and maintenance procedures.

HA overview

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 that these 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 consists of up five FortiManager units of the same FortiManager model and the same firmware version. One of the FortiManager units in the cluster operates as a primary or master unit and the other one to four units operate as backup units. All of the units are visible on the network. The primary unit and the backup units can be at the same location. FortiManager HA also supports geographic redundancy so the primary unit and backup units can be in different locations attached to different networks as long as communication is possible between them (for example over the Internet, over a WAN, or through a private network).

Administrators connect to the primary unit GUI or CLI to perform FortiManager operations. Managed devices connect with the primary unit for normal management operations (configuration push, auto-update, firmware upgrade, and so on). If FortiManager is used to distribute FortiGuard updates to managed devices, managed devices can connect to the primary FortiManager unit or one of the backup units.

If the primary FortiManager unit fails you must manually configure one of the backup units to become the primary unit. The new primary unit will have the same IP addresses as it did when it was the backup unit.

A reboot of the FortiManager device is not required when it is promoted from a slave to the master.

Synchronizing the FortiManager configuration and HA heartbeat

All changes to the FortiManager database are saved on the primary unit, and then these changes are synchronized to the backup units. The FortiManager configuration of the primary unit is also synchronized to the backup units (except for the HA parameters). As a result, the backup units always match the primary unit. So if the primary unit fails, a backup unit can be configured to take the place of the primary unit and continue functioning as a standalone FortiManager unit.

While the FortiManager cluster is operating, all backup units in the cluster exchange HA heartbeat packets with the primary unit so that 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 that 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 received 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 from the HA Status page.

You re-configure 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, you re-configure the cluster by removing the peer IP of the failed backup unit from the primary unit configuration.

Once the cluster is re-configured it will continue to operate as before but with fewer cluster units. If the failed unit is restored you can re-configure 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 another peer IP address, the FortiManager unit assumes the peer is functioning.

When the primary unit is receiving HA heartbeat packets from all of the configured peers or backup units, the primary unit sets the cluster status to up. Once the cluster is up the primary unit then synchronizes its configuration to the backup unit. This synchronization process can take a few minutes depending on the size of the FortiManager database. During this time database and configuration changes made to the primary unit are not synchronized to the backup units. Once synchronization is complete, if changes were made during synchronization, they are re-synchronized to the backup units.

Most of the primary unit configuration, as well as the entire FortiManager database, are synchronized to the backup unit. Interface settings and HA settings are not synchronized. These settings must be configured on each cluster unit.

Once the synchronization is complete, the FortiManager HA cluster begins normal operation.

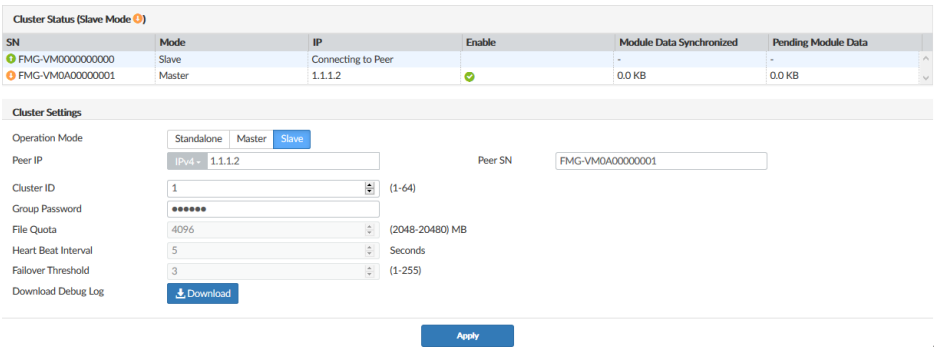
Configuring HA options

To configure HA options go to *System Settings* > *HA*. From here you can configure FortiManager units to start an HA cluster or you can change the HA configuration of the cluster.

To configure a cluster, you must set the mode of the primary unit to master and the modes of the backup units to Slave.

Then you must 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 of the backup unit HA configurations. Also, 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. Because of configuration synchronization you can configure and work with the cluster in the same way as you would work with a standalone FortiManager unit.



Configure the following settings:

Cluster Status	Monitor FortiManagerHA status. See Monitoring HA status on page 345.
SN	The serial number of the device.

	Mode	The high availability mode, either *Master* or *Slave*.
	IP	The IP address of the device.
	Enable	Shows if the peer is currently enabled.
	Module Data Synchronized	Module data synchronized represented in Bytes.
	Pending Module Data	Pending module data represented in Bytes.
Cluster Settings		
	Operation Mode	Select *Master* to configure the FortiManager unit to be the primary unit in a cluster. Select *Slave* to configure the FortiManager unit to be a backup unit in a cluster. Select *Standalone* to stop operating in HA mode.
	Peer IP	Select the peer IP version from the drop-down list, either *IPv4* or *IPv6*. Then, type the IP address of another FortiManager unit in the cluster. For the primary unit you can add up to four Peer IP addresses for up to four backup units. For a backup unit you add the IP address of the primary unit.
	Peer SN	Type the serial number of the FortiManager unit that corresponds to the entered IP address.
	Cluster ID	A number between 1 and 64 that identifies the HA cluster. All members of the HA cluster must have the same cluster ID. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different cluster ID. The FortiManager GUI browser window title changes to include the cluster ID when FortiManager unit is operating in HA mode.
	Group Password	A password for the HA cluster. All members of the HA cluster must have the same group password. The maximum password length is 19 characters. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different password.
	File Quota	Enter the file quota, from 2048 to 20480MB (default: 4096MB). You cannot configure the file quota for backup units.
	Heartbeat Interval	The time in seconds that a cluster unit waits between sending heartbeat packets. The heartbeat interval is also the amount of time that a FortiManager unit waits before expecting to receive a heartbeat packet from the other cluster unit. The default heartbeat interval is 5 seconds. The heartbeat interval range is 1 to 255 seconds. You cannot configure the heartbeat interval of the backup units.

Failover Threshold	The number of heartbeat intervals that one of the cluster units waits to receive HA heartbeat packets from other cluster units before assuming that the other cluster units have failed. The default failover threshold is 3. The failover threshold range is 1 to 255. You cannot configure the failover threshold of the backup units. In most cases you do not have to change the heartbeat interval or failover threshold. The default settings mean that if the a unit fails, the failure is detected after 3 x 5 or 15 seconds; resulting in a failure detection time of 15 seconds. If the failure detection time is too short the HA cluster may detect a failure when none has occurred. For example, if the primary unit is very busy it may not respond to HA heartbeat packets in time. In this situation, the backup unit may assume that 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

The following procedures assume that you are starting with four FortiManager units running the same firmware build and are set to the factory default configuration. The primary unit and the first backup unit are connected to the same network. The second backup units is connected to a remote network and communicates with the primary unit over the Internet.

1. Configure the FortiManager units for HA operation:
   - Configure the primary unit.
   - Configure the backup units.
2. Change the network configuration so that 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. 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 master configuration:

Operation Mode	Master
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. Select *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	Slave
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. Select *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	Slave
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. Select *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 operating HA cluster. The FortiManager HA status dialog box displays information about the role of each cluster unit, the HA status of the

cluster, and also displays 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.

From the FortiManager CLI you can use the command `get system ha` to display the same HA status information.

The following information is displayed:

Cluster Status	The cluster status can be *Up* if this unit is received HA heartbeat packets from all of its configured peers. The cluster status will be *Down* if the cluster unit is not receiving HA heartbeat packets from one or more of its configured peers.
Mode	The role of the FortiManager unit in the cluster. The role can be: • *Master*: for the primary (or master) unit. • *Slave*: 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. During the firmware upgrade procedure, you connect to the primary unit GUI or CLI to upgrade the firmware. Then install the firmware on the slave units.

Similar to upgrading the firmware of a standalone FortiManager unit, normal FortiManager operations are temporarily interrupted while the cluster firmware upgrades. As a result of this interruption, you should upgrade the 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 forwarded to all the slave units, and then all the devices (master and slaves) are rebooted.

   See the *FortiManager Release Notes* and *FortiManager Upgrade Guide* in the Fortinet Document Library for more information.

Administrators may 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 may also be slow, however use the console to connect to the CLI.

Certificates

The FortiManager unit 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 computer that has management access to the FortiManager unit 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 certificates that have expired, been stolen, or otherwise compromised. 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.

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*.

Managing local certificates

You can manage local certificates from the *System Settings* > *Certificates* > *Local Certificates* page. Some options are available on the toolbar. Some options are available in the right-click menu.

Option	Description
Create New	Generate a new certificate signing request.
Delete	Delete the selected local certificate or certificates.
Import	Import a certificate.
View Certificate Detail	View details of the selected local certificate.
Download	Download the selected local certificate to the management computer.

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* window opens.

3. Enter the following information as required:

Certificate Name		The name of the certificate.
Subject Information		• If the unit has a static IP address, select *Host IP* and enter the public IP address of the unit. • If the unit does not have a public IP address, use an email address (or FQDN if available) instead. • If the unit has a dynamic IP address and subscribes to a dynamic DNS service, use a FQDN if available to identify the unit. If you select Domain Name, enter the FQDN of the unit. Do not include the protocol specification (http://) or any port number or path names.
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 (-) icon.
	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 drop-down list.
	E-mail Address (EA)	Contact email address.
	Subject Alternative Name	Optionally, enter one or more alternative names for which the certificate is also valid. Separate names with a comma. A name can be: • e-mail address • IP address • URI • DNS name (alternatives to the Common Name) • directory name (alternatives to the Distinguished Name) You must precede the name with the name type.
Key Type		The key type is set to *RSA*.
Key Size		Select the key size from the drop-down list: *512 Bit*, *1024 Bit*, *1536 Bit*, or *2048 Bit*.
Enrollment Method		The enrollment method is set to *File Based*.

4. Select *OK* to save the certificate request.

Importing local certificates

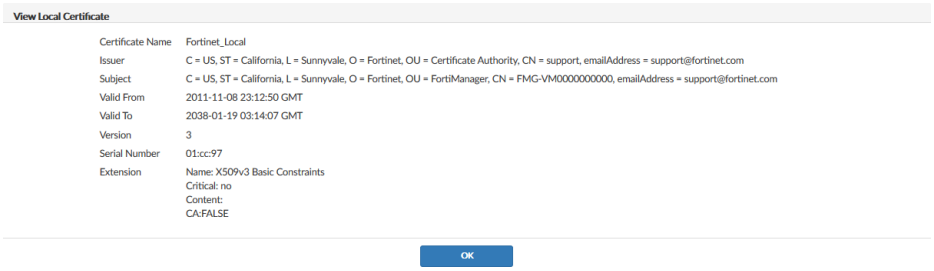
To import a local certificate:

1. Go to *System Settings* > *Certificates* > *Local Certificates*.
2. Click *Import* in the toolbar. The *Import* dialog box opens.
3. Click *Browse...* and locate the certificate file on the management computer
4. Select *OK* to import the certificate.

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 select *View Certificate Detail* in the toolbar. The *Result* page opens.



3. Select *OK* to return to the local certificates list.

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. Select *Import* in the toolbar. The *Import* dialog box opens.
3. Select *Browse...*, browse to the location of the certificate, and select *OK*.

Viewing CA certificate details

To view a CA certificate's details:

1. Go to *System Settings* > *Certificates* > *CA Certificates*.
2. Select the certificates that you would like to see details about, then select *View Certificate Detail* in the toolbar. The *Result* page opens.
3. Select *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 or certificates that you would like to download, select *Download* in the toolbar, 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 that you would like to delete and select *Delete* in the toolbar.
3. Select *OK* in the confirmation dialog box to delete the selected certificate or certificates.

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 certificates that have expired, been stolen, or otherwise compromised. 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. Select *Import* in the toolbar. The *Import* dialog box opens.
3. Select *Browse...*, browse to the location of the CRL, then select *OK* to import it.

Viewing a CRL

To view a CRL:

1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the CRL that you would like to see details about, then select *View Certificate Detail* in the toolbar. The *Result* page opens.
3. When you are finished viewing the CRL details, select *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 that you would like to delete and select *Delete* in the toolbar.
3. Select *OK* in the confirmation dialog box to delete the selected CRL or CRLs.

Fetcher management

Go to *System Settings* > *Fetcher Management* to manage log fetching sessions and profiles.

For more information, see the **Log fetcher management** section in the *FortiAnalyzer Administration Guide*, available in the Fortinet Document Library.

Event log

The event log provides an audit log of actions made by users on FortiManager. The logs created by FortiManager are viewable within the GUI. You can use the *FortiManager Log Message Reference*, available from the Fortinet Document Library to interpret the messages. You can view log messages in the FortiManager GUI that are stored in memory or on the internal hard disk.

Go to *System Settings* > *Event Log* to view the local log list.

The following information is displayed:

#	The log number.
Date Time	The date and time that the log file was generated.
Level	The log level: • Debug • Information • Notification • Warning • Error • Critical • Alert • Emergency
User	User information.

Sub Type	Log sub-type information. The available event subtypes are: System manager event, FortiMail manager event, FG-FM protocol event, Debug I/O log event, Device configuration event, Device manager event, Deployment manager event, Web service event, Real-time monitor event, FortiAnalyzer event, Log and report manager event, Log daemon event, Firmware manager event, FIPS-CC event, FortiGuard service event, Device manager event, FortiClient manager event
Message	Log message details.

The following options are available:

Refresh	Click to refresh the list.
Download	Download the event logs in either CSV or the normal format.
Raw Log / Formatted Log	Click on *Raw Log* to view the logs in their raw state. Click *Formatted Log* to view them in the formatted into a table.
Historical Log	Click to view the historical logs list.
View	View the selected log file. This option is only available when viewing historical event logs.
Delete	Delete the selected log file. This option is only available when viewing historical event logs.
Clear	Clear the selected file of logs. This option is only available when viewing historical event logs.

Type	Select the type from the drop down list. This option is only available when viewing historical logs. Select one of the following: *Event Log*, *FDS Upload Log*, or *FDS Download Log*. When selecting *FDS Upload Log*, select the device from the drop-down list. When selecting *FDS Download Log*, select the service (*FDS*, *FGD*, or *FCT*) from the *Service* drop-down list, select the event type (*All Event*, *Push Update*, *Poll Update*, or *Manual Update*) from the *Event* drop-down list, then select *Go* to browse logs.
Search	Enter a search term to search the historical logs. This option is only available when viewing historical event logs.
Pagination	Use these page options to browse logs and adjust how many logs are shown per page.

Task monitor

Using the task monitor, you can view the status of the tasks that you have performed.

Go to *System Settings* > *Task Monitor*, then select a task category from the *View* field drop-down list, or leave as the default *All*. Select a column header to sort the table by that column.

The following information is displayed:

ID	The identification number for a task.
Source	The platform from where the task is performed. The source includes the following: Package Clone, Import Wizard, System checkpoint, Install Configuration, Device Manager.
Description	The nature of the task.
User	The users who have performed the tasks.

Status	The status of the task (hover over the icon to view the description): • *All*: All types of tasks. • *Done*: Completed with success. • *Error*: Completed without success. • *Cancelled*: User cancelled the task. • *Cancelling*: User is cancelling the task. • *Aborted*: The FortiManager system stopped performing this task. • *Aborting*: The FortiManager system is stopping performing this task. • *Running*: Being processed. In this status, a percentage bar appears in the Status column.
Start Time	The date and time that the task was performed.
ADOM	The ADOM to which the task applies.

The following options are available:

Delete	Remove the selected task or tasks from the list. This becomes *Cancel Running Task(s)* when *View* is *Running*.
View	Select which tasks to view from the drop-down list, based on their status. The available options are: *Running*, *Pending*, *Done*, *Error*, *Cancelling*, *Cancelled*, *Aborting*, *Aborted*, *Warning*, and *All*. Default: All
Expand Arrow	In the *Source* column, select the expand arrow icon to display the specific actions taken under this task. To filter the specific actions taken for a task, select one of the options on top of the action list. Select the history icon to view specific information on task progress. This can be useful when troubleshooting warnings and errors.
Group Error Devices	Select *Group Error Devices* to create a group of the devices that failed, allowing for re-installations to easily be done on only the failed devices.
History	Click the history icon to view task details in a new window.
Pagination	Browse pages in the task monitor page. You can select the number of task entries to display from the drop-down menu.

Configuring the task list size

To configure the task list size:

1. Go to *System Settings* > *Advanced* > *Advanced Settings* .
2. In the *Task List Size* field, type the maximum number of tasks to retain, then select *Apply*.

Advanced

The *System Settings* > *Advanced* menu enables you to configure SNMP, meta field data, and other settings. The following options are available:

SNMP	Select to configure FortiGate and FortiManager reporting through SNMP traps.
Mail server	Select to configure mail server settings for alerts, edit existing settings, or delete mail servers.
Syslog server	Select to configure syslog server settings for alerts, edit existing settings, or delete syslog servers.
Meta fields	Select to configure metadata fields for FortiGate objects, and for FortiGate-5000 series shelf managers.
Device log settings	Select to configure log settings and access. This menu is available when *FortiAnalyzer Features* is enabled.
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. This menu is available when *FortiAnalyzer Features* is enabled.
Advanced settings	Select to configure global advanced settings such as offline mode, device synchronization settings and install interface policy only.

SNMP

SNMP is a method for a FortiManager system to monitor and report on FortiGate devices. It also can allow you to monitor a FortiManager system on your local computer. You will need an SNMP agent on your computer to read the SNMP information.

Using SNMP, your FortiManager system checks the attached FortiGate devices for their system health, traffic levels, and many other details. By default when a FortiGate device is initially configured on your FortiManager system, that FortiGate device's SNMP settings are configured to report to the FortiManager system.

Go to *System Settings* > *Advanced* > *SNMP* to configure your FortiManager system's SNMP settings.

SNMP has two parts - the SNMP agent or the device that is sending traps, and the SNMP manager that monitors those traps. The SNMP communities on the monitored FortiGate devices are hard coded and configured by the FortiManager system - they are not user configurable.

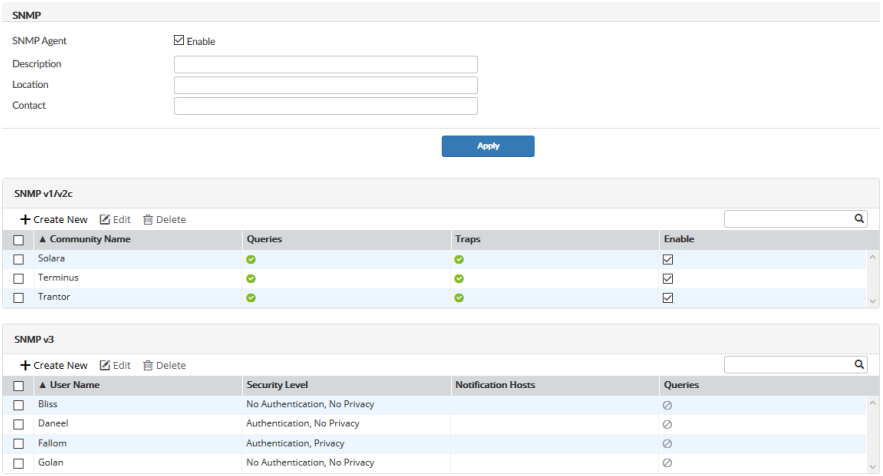
The FortiManager SNMP implementation is read-only — SNMP v1, v2c, and v3 compliant SNMP manager applications, such as those on your local computer, have read-only access to FortiManager system information and can receive FortiManager system traps.

Configuring the SNMP agent

The SNMP agent sends SNMP traps that originate on the FortiManager system to an external monitoring SNMP manager defined in one of the FortiManager SNMP communities. 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.



The following information and options are available:

SNMP Agent	Select to enable the FortiManager SNMP agent. When this is enabled, it sends FortiManager SNMP traps.
Description	Type a description of this FortiManager system to help uniquely identify this unit.
Location	Type the location of this FortiManager system to help find it in the event it requires attention.
Contact	Type the contact information for the person in charge of this FortiManager system.
SNMP v1/2c	The list of SNMP v1/v2c communities added to the FortiManager configuration.
Create New	Select *Create New* to add a new SNMP community. If SNMP agent is not selected, this control will not be visible.
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	Select to enable or deselect to disable the SNMP community.
SNMP v3		The list of SNMPv3 users added to the configuration.
	Create New	Select *Create New* to add a new SNMP community. If SNMP agent is not selected, this control will not be visible. For more information, see Configuring a SNMPv3 user on page 359.
	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 that query is enabled. The disabled icon indicates query is disabled.

Configuring an SNMP v1/v2c community

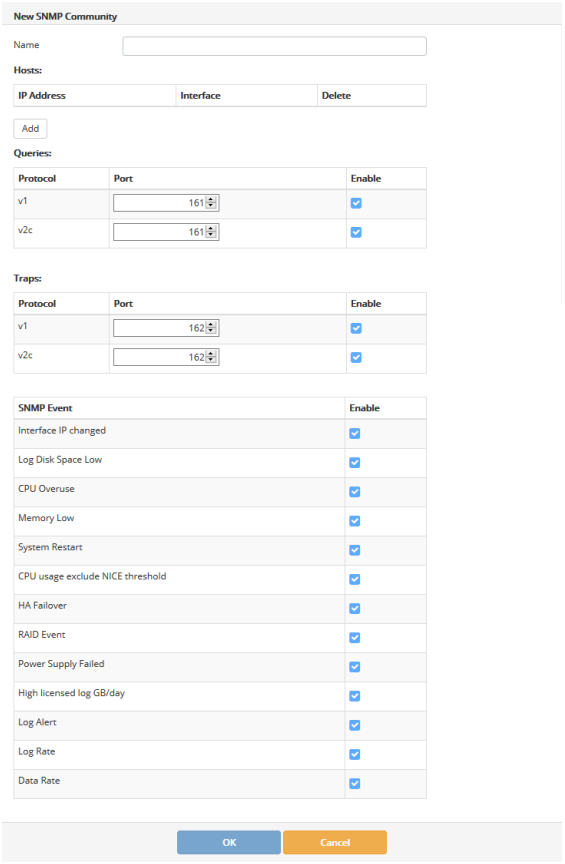
An SNMP community is a grouping of equipment for network administration purposes. Add SNMP communities so that the FortiManager system (the SNMP agent in this case) can connect to the SNMP manager that is monitoring.

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.

Select *Create New* in the SNMP v1/v2c toolbar to open the *New SNMP Community* page, where you can configure a new SNMP community.

When you create a new SNMP community, there are no host entries. Selecting *Add* creates an entry that broadcasts the SNMP traps and information to the network connected to the specified interface.



Configure the following settings:

Name		Type a name to identify the SNMP community. If you are editing an existing community, you will be unable to change the name.
Hosts		The list of hosts that can use the settings in this SNMP community to monitor the FortiManager system. Select *Add* to create a new entry that you can edit.
	IP Address	Type the IP address of an SNMP manager. By default, the IP address is 0.0.0.0 so that any SNMP manager can use this SNMP community.
	Interface	Select the name of the interface that connects to the network where this SNMP manager is located from the drop-down list. You need to do this if the SNMP manager is on the Internet or behind a router.
	Delete	Select the delete icon to remove this SNMP manager entry.
	Add	Select to add a new default entry to the Hosts list that you can edit as needed. You can have up to eight SNMP manager entries for a single community.

Queries	Type the port number that the FortiManager system uses to send SNMPv1 and SNMPv2c queries to the FortiManager in this community. Enable queries for each SNMP version that the FortiManager system uses. Default port: 161
Traps	Type the Remote port number that the FortiManager system uses to send SNMPv1 and SNMPv2c traps to the FortiManager in this community. Enable traps for each SNMP version that the FortiManager system uses. Default port: 162
SNMP Event	Enable the events that will cause the FortiManager unit to send SNMP traps to the community. FortiManager SNMP events: • *Interface IP changed* • *Log disk space low* • *CPU Overusage* • *Memory Low* • *System Restart* • *CPU usage exclude NICE threshold* • *HA Failover* • *RAID Event* (only available for devices that support RAID) • *Power Supply Failed* FortiAnalyzer feature set SNMP events: • *High licensed device quota* • *High licensed log GB/day* • *Log Alert* • *Log Rate* • *Data Rate*

Configuring a SNMPv3 user

The FortiManager SNMPv3 implementation includes support for queries, traps, authentication, and privacy. Select *Create New* in the SNMPv3 toolbar to open the *New SNMP User* page, where you can configure a new SNMP user. You can also edit and delete existing SNMPv3 users.

Configure the following settings:

User Name	The name of the SNMPv3 user.
Security Level	The security level of the user: • *No Authentication, No Privacy* • *Authentication, No Privacy*: Select the authentication algorithm (*SHA1*, *MD5*) and enter the password. • *Authentication, Privacy*: Select the authentication algorithm (*SHA1*, *MD5*), the private algorithm (*AES*, *DES*) and enter the password.

Notification Hosts	The IP address or addresses of the host. Select the add icon to add multiple IP addresses.
Queries	Select to enable queries, then enter the port number (default: 161).
SNMP Event	Enable the events that will cause the FortiManager unit to send SNMP traps to the community. FortiManager SNMP events: • *Interface IP changed* • *Log disk space low* • *CPU Overusage* • *Memory Low* • *System Restart* • *CPU usage exclude NICE threshold* • *HA Failover* • *RAID Event* (only available for devices that support RAID) • *Power Supply Failed* FortiAnalyzer feature set SNMP events: • *High licensed device quota* • *High licensed log GB/day* • *Log Alert* • *Log Rate* • *Data Rate*

SNMP MIBs

Fortinet device SNMP agents support Fortinet proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiManager unit configuration.

RFC support for SNMP v3 includes Architecture for SNMP Frameworks (RFC 3411), and partial support of User-based Security Model (RFC 3414).

The Fortinet and FortiManager MIBs are listed in SNMP MIBs along with the two RFC MIBs. You can obtain these MIB files from Customer Service & Support. To be able to communicate with the SNMP agent, you must compile 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.

You can download the FortiManager MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager 5.00 file folder.

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. For more information, see and Fortinet & FortiManager MIB fields on page 362.
FORTINET-FORTIMANAGER-MIB.mib	The proprietary FortiManager MIB includes system information and trap information for FortiManager units.
RFC-1213 (MIB II)	The Fortinet SNMP agent supports MIB II groups with the following exceptions. • No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all Fortinet traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB.
RFC-2665 (Ethernet-like MIB)	The Fortinet SNMP agent supports Ethernet-like MIB information with the following exception. No support for the dot3Tests and dot3Errors groups.

SNMP traps

Fortinet devices share SNMP traps, but each type of device also has traps specific to that device. 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 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:
	`config system snmp sysinfo`
	`set trap-high-cpu-threshold <percentage value>`
	`end`

Trap message	Description

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:
	`config system snmp sysinfo`
	`set trap-cpu-high-exclude-nice-threshold <percentage value>`
	`end`

Memory low (fnTrapMemThreshold)	Memory usage exceeds 90 percent. This threshold can be set in the CLI using the following commands:
	`config system snmp sysinfo`
	`set trap-low-memory-threshold <percentage value>`
	`end`

Log disk 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. Not available on all models. Available on some devices which 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 (fmTrapHASwitch)	FortiManagerHA cluster has been re-arranged. A new master has been selected and asserted.

Fortinet & FortiManager MIB fields

The Fortinet MIB contains fields reporting current Fortinet unit status information. The tables below list the names of the MIB fields and describe the status information available for each one. You can view more details about the information available from all Fortinet MIB fields by compiling the fortinet.3.00.mib file into your SNMP manager and browsing the Fortinet MIB fields.

System MIB fields:

MIB field	Description
fnSysSerial	Fortinet unit serial number.

Administrator accounts:

MIB field	Description	
fnAdminNumber	The number of administrators on the Fortinet unit.	
fnAdminTable	Table of administrators.	
	fnAdminIndex	Administrator account index number.
	fnAdminName	The user name of the administrator account.
	fnAdminAddr	An address of a trusted host or subnet from which this administrator account can be used.
	fnAdminMask	The netmask for fnAdminAddr.

Custom messages:

MIB field	Description
fnMessages	The number of custom messages on the Fortinet unit.

MIB fields and traps

MIB field	Description
fmModel	A table of all FortiManager models.
fmTrapHASwitch	The FortiManager HA cluster has been re-arranged. A new master has been selected and asserted.

Mail server

Configure SMTP mail server settings for event management, edit existing settings, or delete mail servers. To view and configure mail servers, go to *System Settings* > *Advanced* > *Mail Server*.

If an existing mail server is used in an event handler, the delete icon is removed and the mail server entry cannot be deleted.

To create a new mail server, select *Create New* in the toolbar, configure the following settings, then Select *OK*.

SMTP Server Name	Enter a name for the SMTP server.
SMTP Server	Enter the SMTP server domain information, e.g. mail@company.com.

SMTP Server Port	Enter the SMTP server port number. Default port: 25
Enable Authentication	Select to enable authentication.
Email Account	Type an email account, e.g. administrator@company.com.
Password	Type the email account password.

To edit a mail server:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Either right-click and select the *Edit* from the menu, double-click on the server, or select a server then click *Edit* in the toolbar.
3. Edit the settings as required, and then select *OK* to apply the changes.

To test the mail server:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Either select an entry in the list then click *Test* from the toolbar, or right-click a server then select *Test* from the menu.
3. Type the email address that you would like to send a test email to and select *OK*. A confirmation or failure message will be displayed.
4. Select *OK* to close the confirmation dialog box.

To delete a mail server:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Either select a server then click *Delete* in the toolbar, or right-click a server then select *Delete* in the menu.
3. Select *OK* in the confirmation box to delete the server.

Syslog server

Configure syslog server settings for alerts, edit existing settings, or delete syslog servers.

If an existing syslog server is used in an event handler, the delete icon is removed and the syslog server entry cannot be deleted.

To view and configure syslog servers, go to *System Settings* > *Advanced* > *Syslog Server*.

To create a new syslog server, select *Create New* in the toolbar, configure the following settings, then Select *OK*.

Name	Type a name for the syslog server.
IP address (or FQDN)	Type the IP address or FQDN of the syslog server.
SMTP Server Port	Type the syslog server port number. Default port: 514

To edit a syslog server:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Either right-click and select the *Edit* from the menu, double-click on the server, or select a server then click *Edit* in the toolbar.
3. Edit the settings as required, and then select *OK* to apply the changes.

To test the syslog server:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Either select an entry in the list then click *Test* from the toolbar, or right-click a server then select *Test* from the menu. A confirmation or failure message will be displayed.

To delete a syslog server:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Either select a server then click *Delete* in the toolbar, or right-click a server then select *Delete* in the menu.
3. Select *OK* in the confirmation box to delete the server.

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.

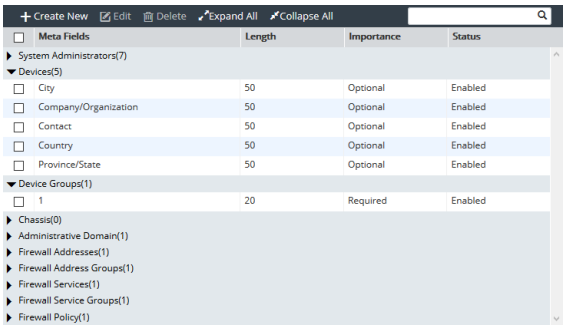
With the fields set as mandatory, administrators must supply additional information when they create a new FortiGate object, such as an administrator account or firewall policy. Fields for this new information are added to the FortiGate unit dialog boxes in the locations where you create these objects. You can also provide fields for optional additional information.

The one exception to this is the Administrators system object. This object applies only to administrators on the FortiManager unit. All other objects are related to FortiGate units.

Managing meta fields

You can create, edit, and delete metadata fields from the *System Settings* > *Advanced* > *Meta Fields* page. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a meta field to display the menu.

Option	Description
Create New	Create new meta fields.
Edit	Edit the selected meta field.
Delete	Delete the selected meta field.



To create a new meta field:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Select *Create New* from the toolbar. The *Add Meta-field* dialog box opens.
3. Configure the following settings:

Object	The object to which this metadata field applies: *System Administrators*, *Devices*, *Device Groups*, *Chassis*, *Administrative Domain*, *Firewall Addresses*, *Firewall Address Groups*, *Firewall Services*, *Firewall Service Groups*, or *Firewall Policy*.
Name	Enter a label to use for the field.
Length	Select the maximum number of characters allowed for the field from the drop-down list (*20*, *50*, or *255*).
Importance	Select *Required* to make the field compulsory, otherwise select *Optional*.
Status	Select *Disabled* to disable this field. This field is only available for non-firewall objects. The default setting is *Enabled*.

4. Select *OK* to save the new field.

To edit a meta field:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Either right-click on the name of the meta field that you need to edit then select *Edit* from the menu, or select the field then select *Edit* from the toolbar.
3. Select *OK* to apply the changes.

Only the length, importance, and status can be edited.

To delete meta fields:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Either select the meta fields that you would like to delete then select *Delete* from the toolbar, or right-click a field and select *Delete* from the menu.
3. Select *OK* in the confirmation box to delete the selected fields.

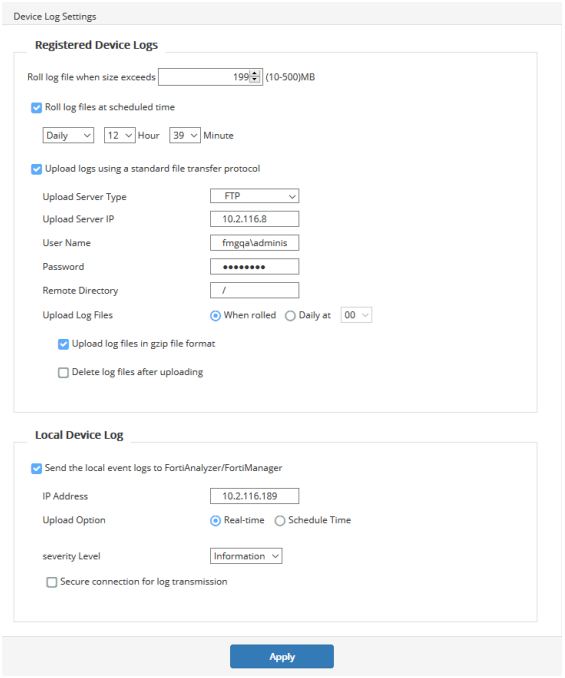
The default meta fields cannot be deleted.

Device log settings

The FortiManager allows you to log system events to disk. The device log settings menu allows you to configure event logging, log rollover, and upload options.

This feature is available in the GUI when *FortiAnalyzer Features* is enabled. For more information, see Enable or disable FortiAnalyzer features on page 334.

To configure log settings, go to *System Settings* > *Advanced* > *Device Log Setting*.



Configure the following settings and then select *Apply*:

Registered Device Logs	
Roll log file when size exceeds	Enter the log file size. • Range: 10 to 500 MB • Default: 200 MB
Roll log files at a regular time	Select to roll logs daily or weekly. When selecting daily, select the hour and minute value in the drop-down lists. When selecting weekly, select the day, hour, and minute value in the drop-down lists.

Upload logs using a standard file transfer protocol	Select to upload logs and configure the following settings.
Upload Server Type	Select one of *FTP*, *SFTP*, or *SCP*.
Upload Server IP	Enter the IP address of the upload server.
User Name	Select the username that will be used to connect to the upload server.
Password	Select the password that will be used to connect to the upload server.
Remote Directory	Select the remote directory on the upload server where the log will be uploaded.
Upload Log Files	Select to upload log files when they are rolled according to settings selected under *Roll Logs* or daily at a specific hour.
Upload rolled files in gzipped 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 drop-down list. This option is only available when *Upload Option* is *Realtime*.
Secure connection for log transmission	Select to use a secure connection for log transmission.

Configuring rolling and uploading of logs using the CLI

You can control device log file size and 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.

Configure the time to be either a daily or weekly occurrence, and when the roll occurs. 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-2012-09-29-08-03-54.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 CLI. For more information, see the *FortiManager CLI Reference*.

To enable or disable log file uploads:

To enable log uploads, enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set upload enable
      end
   end
```

To disable log uploads, enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set upload disable
      end
   end
```

To roll logs when they reach a specific size:

Enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set file-size <integer>
      end
   end
```

where `<integer>` is the size at which the logs will roll, in MB.

To roll logs on a schedule:

To disable log rolling, enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set when none
      end
   end
```

To enable daily log rolling, enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set upload enable
      set when daily
      set hour <integer>
      set min <integer>
      set file-size <integer>
      end
   end
```

where:

`hour <integer>`	The hour of the day when the FortiManager rolls the traffic analyzer logs.
`min <integer>`	The minute when the FortiManager rolls the traffic analyzer logs.
`file-size <integer>`	Roll log files when they reach this size (MB).

To enable weekly log rolling, enter the following CLI commands:

```
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
   end
```

where:

`days {mon | tue | wed | thu | fri | sat | sun}`	The days week when the FortiManager rolls the traffic analyzer logs.
`hour <integer>`	The hour of the day when the FortiManager rolls the traffic analyzer logs.
`min <integer>`	The minute when the FortiManager rolls the traffic analyzer logs.

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.

To configure automatic deletion settings, go to *System Settings* > *Advanced* > *File Management*.

This feature is available in the GUI when *FortiAnalyzer Features* is enabled. For more information, see Enable or disable FortiAnalyzer features on page 334.

For each settings, the number of *Hours*, *Days*, *Weeks*, or *Months* after which the content will be deleted must be configured after the setting has been enabled. The following settings can be enabled and configured:

- Device log files older than
- Quarantined files older than

- Reports older than
- Content archive files older than

Advanced settings

To view and configure advanced settings options, go to the *System Settings* > *Advanced* > *Advanced Settings* page. The *Advanced Settings* dialog box opens.

Configure the following settings and then select *Apply*:

Offline Mode	Enabling *Offline Mode* shuts down the protocol used to communicate with managed devices. This is a feature you can use to troubleshoot problems, allowing you to change FortiManager unit settings without affect managed devices.FortiManager cannot automatically connect to FortiGate if offline mode is enabled.
ADOM Mode	Select the ADOM mode, either *Normal* or *Advanced*. Advanced mode will allow you to assign a VDOM from a single device to a different ADOM, but will result in more complicated management scenarios. It is recommended only for advanced users.
Download WSDL file	Select the required WSDL functions and select the *Download* button to download the WSDL file to your management computer. When selecting *Legacy Operations*, no other options can be selected. Web services is a standards-based, platform independent, access method for other hardware and software APIs. The file itself defines the format of commands the FortiManager will accept as well as the response 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 administrative user would from the GUI or CLI. For more information, see the *FortiManager XML API Reference*.
Chassis Management	Enable chassis management, then enter the chassis update interval: 4 to 1440 minutes; default: 15 minutes.
Configuration Changes Received from FortiGate	Select to either automatically accept changes or to prompt the administrator to accept the changes.
Task List Size	Set a limit on the size of the task list.
Verify Installation	Select to preview the installation before proceeding.
Allow Install Interface Policy Only	Select to manage and install interface based policies only 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 *Policy Packages* and *Object Configurations* tabs on a single pane in the *Policy & Objects* module. See Display options on page 191.