FORTINET
UNIFIED THREAT MANAGEMENT SOLUTIONS

FortiManager™

Version 4.0 MR2

Administration Guide

FortiManager Administration Guide

Version 4.0 MR2

November 12, 2010

02-42002-92196-20101112

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet®, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Regulatory compliance

FCC Class A Part 15 CSA/CUS

Caution: Risk of Explosion if Battery is replaced by an Incorrect Type. Dispose of Used Batteries According to the Instructions.

Contents

What's New for 4.2

This section describes some of the new features and changes in FortiManager 4.0 MR2.

Note: This document is a work in progress and may not reflect fully the features in the product due to the developmental state of the firmware.

Manage FortiGuard updates

This feature allows you to control when FortiGuard updates are propagated to managed devices. This can be useful to offload updates to outside of office hours to prevent potentially slowing down your network.

In the root ADOM, go to *System Settings* > *FortiGuard Center* > *Update* mode to set either Automatic, Delay, or Manual. If *Delay*, you select the duration of the delay in minutes. See "FortiGuard Center" on page 79.

GUI changes

FortiManager 4.2 includes a number of GUI changes designed to improve the usability of the web-based interface.

Breadcrumbs

Breadcrumbs, also known as navigation history, displays the sequence of items you selected to reach your current display. This allows you to easily jump back to any point along that path for easier navigation. This area also displays a home icon to return to the top level and a lock icon to display if a device is locked or unlocked. See "Breadcrumbs" on page 82.

Drag-and-drop, Right-click menus

The ability to right-click on items such as policy objects as well as extended cut, paste, and copy have been added to Global Objects, and Security Console. The behavior is similar to a typical desktop environment where you have extended options when you right-click on an object. This feature is useful when managing large amounts of data such as reordering a list of 100 policies or copying table data. See "Common configuration actions" on page 125, and "Dynamic Objects" on page 206.

Another new feature is the ability to drag-and-drop an item in a list. Select an item in a list by left-clicking and holding the button down, drag the item to a new location in the list, and drop it by releasing the mouse button.

GUI Frame Consolidation

Improvements to the GUI layout are designed to maximize the available space in the right frame where the data is displayed and managed. This was accomplished by consolidating the left and middle frames, and shortening the top frame where the Main Menu Bar icons are located.

Previously tabs were used at the top of the Content Pane for navigation, as well as extended options opening up a middle pane between the left and right panes. Both of these were moved into the left pane for easier navigation. See "Web-based manager" on page 25.

ELBC GUI improvements

Extended Load Balancing Cluster (ELBC) management GUI has improved for 4.2. It displays ELBC clusters as blades in a Chassis, treating it like a single device instead of the multiple cards that are part of the cluster.

FortiAnalyzer GUI updates

FortiAnalyzer GUI has improved for 4.2. It is easier to add a FortiAnalyzer and connect to it through the FortiManager.

Security Console

In FortiManager 4.2 the Security Console has had a number of changes designed to improve the ease of use of its features.

Copy from Device

An extension to the Global Object and Security Console Policy Console modules that allows policies to be imported from a device to the global policy table. Using this method an administrator can use an already configured FortiGate device as a template, import policies from that unit, and then push them out to other units to ensure a uniform configuration with minimal effort. See "Copy a global object from a device" on page 125.

Policy CSV Export

Allow policy table to be exported in comma-separated-value (CSV) format, which can be imported by Excel or other applications. This feature is useful when exporting policies for external review such as for a compliance audit. See "Policy Console" on page 199.

Usability

Load Balancing is now a separate category under Policy Objects in GMS mode. Previously it was part of Virtual IP.

When the Security Console window is detached, selecting Save takes you to the revision history screen to allow you to save or import revisions.

Right-click menu actions have been added to the Global objects, and Security Console. See "Security Console" on page 197.

Configuration change highlights

In GMS mode, making a change under Security Console will result in that change being highlighted and flagged in the GUI. This helps you quickly see what changes have recently been made to the security console, and what changes are pending.

Importing and exporting configurations is easier. This allows administrators to more easily reuse parts of configurations many times. This saves time and decreases configuration errors. See "Security Console" on page 197.

New devices supported

New FortiGate models are supported in FortiManager 4.2 including FGT-ONE, FGT-200B, and FGT-1240B. FortiOS 4.2 is also supported.

Global database policy header / footer in EMS mode

A new feature for EMS Mode allows the definition of Global Policies. Header policies are firewall policies that are located at the top of the list and will be checked first. Footer policies are located at the bottom of the policy list and will be checked last. This is useful to ensure similar behavior in all managed devices, and group policies according to their location and intended use. See "Configuring firewall policies" on page 129.

Radius secondary server

Added support for a secondary Radius Server. This is for administrator authentication redundancy in the event the primary Radius server is unavailable. See "RADIUS server" on page 66

FortiClient Manager – Active Directory OU Integration

FortiClient Manager allows integration with MS Active Directory (AD) groupings to setup FortiClient (FCT) groups. See "Working with Windows AD users and groups" on page 335.

Introduction

The FortiManager system is an integrated platform for centralized management of the major Fortinet products.

Using the FortiManager system, you can:

- configure multiple FortiGate units, FortiSwitch units, FortiOS Carrier units, FortiMail units, FortiAnalyzer units, and FortiClient PCs,
- configure and manage VPN policies,
- monitor the status of these units,
- view and analyze device logs,
- update the virus and attack signatures,
- provide web filtering and antispam service to the licensed devices as a local Fortinet Distribution Network (FDN) server.
- update the firmware images of the devices.

The FortiManager system scales to manage up to a thousand devices and FortiClient PCs simultaneously. It is designed for large enterprises and managed security service providers. FortiManager system architecture emphasizes reliability, scalability, ease of use, and easy integration with third-party systems.

This section contains the following topics:

About the FortiManager system

The FortiManager system is a security-hardened appliance with simplified installation, and improved system reliability and security. You can install a second peer FortiManager system for database backups.

The FortiManager system manages communication between the managed devices and the FortiManager web-based manager.

The FortiManager system stores and manages all managed devices' configurations.

It can also act as an on-site FortiGuard Network (FDN) server for the managed devices to download virus and attack signatures, and to use the web filtering and antispam service. This will significantly reduce the network delay and usages, compared with the managed devices' connection to an FDN server over the Internet.

Configuration and installation workflow

The FortiManager system maintains a global database represented by *Global Objects/Security Console*, a device database represented by a device's *Configuration* tab, and a configuration repository represented by a device's *Revision History* tab. For more information, see "Device Manager pane" on page 217 and "Managing configuration revision history" on page 278.

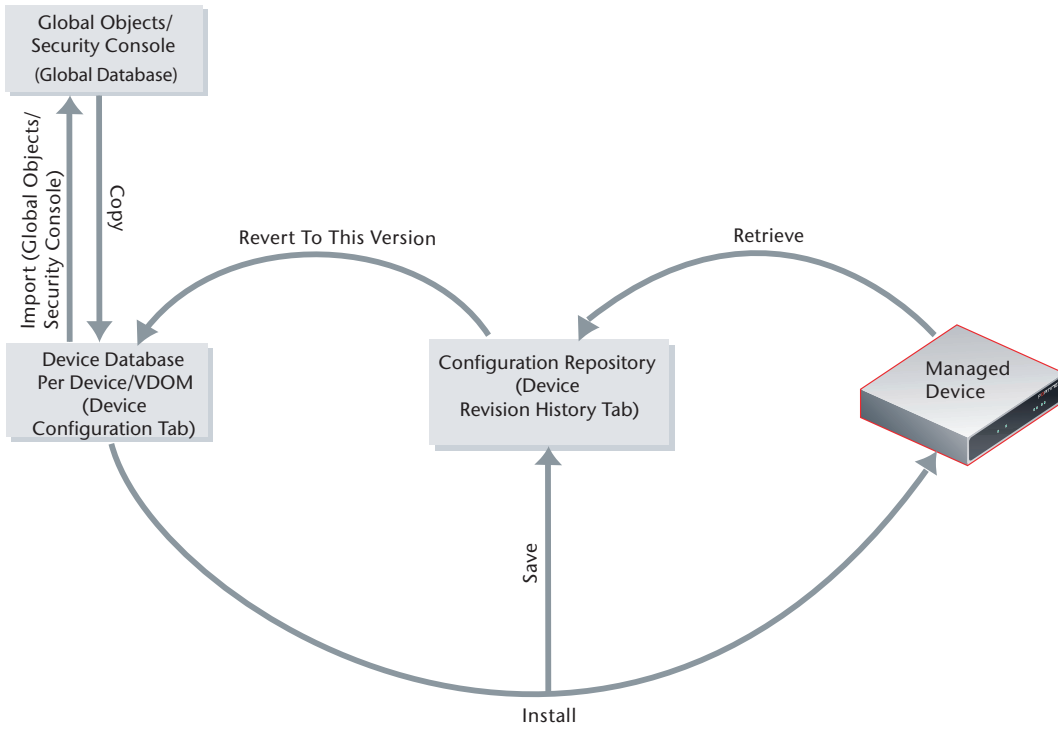
The global database provides a central place where you can configure global objects and copy the configurations to the device database for a selected device or a group of devices.

The device database saves configurations made to a device, copied from the global database, and checked out from the configuration repository.

The configuration repository acts as a revision control system. Configuration files taken from the managed devices are saved in this repository. You can check out the configuration files from the repository and modify them as needed before checking them back into the repository. When you install a configuration file to the devices, the file is also checked out from the repository.

The following diagram shows how managed devices interact with the FortiManager system, especially how all of the installation and configuration features interact with each other and what the specific commands accomplish.

Figure 1: Configuration and installation workflow



Copy	This *Copy* icon, under most objects in the *Global Objects/Security Console,* is used to copy the global object to a device or device group saved in the FortiManager device database. For more information, see "To copy a global object" on page 127.
Import	This *Import* icon, under most objects in the *Global Objects/Security Console*, is used to get a global object from a device saved in the FortiManager device database to the global database. For more information, see "To import a global object" on page 125.
Revert to this version	This icon, under the *Revision History* tab of a device, takes a configuration version from the repository and moves it to the *Configuration* tab, where you can edit it as needed. Once you have made the required changes, use *Install* in the Main Menu Bar to save the new configuration in the repository with a new version number and install it to the selected device(s). For more information, see "Configuring Devices" on page 217.
Retrieve	The *Retrieve* button, under the *Revision History* tab of a device, allows you to get the actual configuration version that is currently running on the managed device and save it to the FortiManager repository. When the configuration version on the device and the configuration version in the FortiManager repository are the same, the unit(s) are synchronized. This synchronization is indicated under device status. For more information, see "Managing configuration revision history" on page 278.
Install	*Install* in the Main Menu Bar installs a configuration version to the selected device(s)/group(s) and saves the configuration to the FortiManager repository with a new version number at the same time. For more information, see "Installing Device Configurations" on page 277.

Management tools

There are three ways to manage and configure the FortiManager system and/or the devices that it manages.

Web-based manager

You can use the FortiManager web-based manager to manage and configure FortiGate units, FortiMail units, FortiAnalyzer units, and FortiClient PCs as well as to view unit configuration, status, system health, and real time logs. The FortiManager web-based manager supports role-based administration. Permissions and device access can be set individually for each manager account added to the FortiManager web-based manager.

Administrators with read and write access can view the configuration, health status and logs, and can change the configurations of the managed devices assigned to them. The FortiManager web-based manager also allows these users to remotely upgrade FortiGate unit firmware and virus and attack definitions.

Command Line Interface

You can also use the Command Line Interface (CLI) to access and manage the FortiManager system and other devices that it manages.

For detailed information about using the CLI, see the *FortiManager CLI Reference*.

The control buttons and LCD

You can use the control buttons and LCD of the FortiManager system to configure the FortiManager system IP address and netmask.

For detailed information about using the control buttons and LCD, see the *FortiManager Installation Guide*.

About this document

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

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

This document contains the following information:

- What's New for 4.2 lists and describes some of the new features and changes in FortiManager 4.0 MR2.
- Web-based manager introduces the FortiManager web-based manager tool that is used to manage and configure FortiGate units and FortiClient PCs and to view FortiGate unit configuration, device status, system health, real time logs, and historical logs.
- Administrative Domains describes ADOMs that can define sets of devices to be controlled by one or more administrators.
- System Settings describes how to control and monitor the operation of the FortiManager system, including network settings, firmware changes, configuration backup and administrator access.
- Managing Devices describes adding devices to the FortiManager system.
- Global Objects provides a central place where you can configure group level objects and install the configurations to an individual device or a group of devices.
- Security Console provides central configuration of VPNs and firewall policies.
- Administrative Web Portal describes how to create administrative web portals for small customers who have only one FortiGate unit or even just one VDOM on a FortiGate unit.
- Configuring Devices describes configuring the devices added to the FortiManager system.
- Working with Scripts describes how to manage scripts from devices that are in operation. Administrators can use functions, such as the configure function, the debug function, the show function, and the get function, to manage devices using scripts.
- Using FortiGuard services describes how to use the FortiManager system as a local update server for AV/IPS signatures and a on-site FDN server for web filtering and antispam services.
- Changing Firmware describes how to update device firmware images.
- Installing Device Configurations describes installing configuration changes to the devices and pulling the existing configurations from the devices.
- Real-Time Monitor describes how to monitor the status of a number of devices at a glance.
- FortiAnalyzer Devices enables you to browse log files and log messages, including configuring log settings for your managed devices.
- FortiClient Manager describes how to use the FortiClient Manager to centrally manage FortiClient software running on PCs (FortiClient PCs).
- FortiManager HA describes using the server high availability feature.

- Managing Firmware Versions includes upgrading issues for all FortiManager 3.0 firmware versions and how to revert back to a previous firmware version, either to FortiManager 2.80 MR10 or an earlier FortiManager 3.0 firmware maintenance release.

Order of operation

If you have just installed the FortiManager system, start with "System Settings" on page 41. Otherwise the basic order that you should use the FortiManager system is as follows:

1. Add devices. See "Managing Devices" on page 81.
2. Configure devices. See "Configuring Devices" on page 217, "Global Objects" on page 121, and "Security Console" on page 197.
3. Install configuration changes to the devices. See "Installing Device Configurations" on page 277.
4. Update device firmware, AV and IPS signatures. See "Using FortiGuard services" on page 249.
5. Monitor devices. See "Real-Time Monitor" on page 283.
6. Manage device logs. See "FortiAnalyzer Devices" on page 299.
7. Configure system settings. See "System Settings" on page 41.
8. Use the FortiClient Manager to add, delete and configure FortiClient PCs. See "FortiClient Manager" on page 303.

Document conventions

The following document conventions are used in this guide:

- In the examples, private IP addresses are used for both private and public IP addresses.
- Notes and Cautions are used to provide important information:

Note: Highlights useful additional information.

Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

Typographic conventions

Fortinet documentation uses the following typographical conventions:

Table 1: Typographic conventions

Convention	Example
Menu commands	Select *Device Manager* > *Group* from the Main Menu Bar to create a device group.
Keyboard input	Select *Create New*, and enter the name `myFortiGate`.

Code examples	`config fmsystem adminsetting`
	`set verify_serial_number enable`
	`end`

CLI command syntax	`config router static`
	`edit 1`
	`set device "port1"`
	`set gateway 172.20.120.2`
	`next`
	`end`

Document names	*FortiManager Administration Guide*
File content	<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>
Program output	`Welcome!`
Variables	`<hostname>`

FortiManager documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at http://docs.forticare.com.

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 FortiGate units, FortiMail units, FortiAnalyzer units, and FortiClient PCs. It includes information on how to configure multiple FortiGate units, FortiAnalyzer units, and FortiClient PCs, 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 antispam service to the licensed FortiGate units as a local Fortinet Distribution Network (FDN) server, and updating the firmware images of the managed FortiGate units.

- *FortiManager System QuickStart Guide*

  This document is included with your FortiManager system package. Use this document to install and begin working with FortiManager system and FortiManager web-based manager.

- *FortiManager online help*

  You can get online help from the FortiManager web-based manager. FortiManager online help contains detailed procedures for using the FortiManager web-based manager to configure and manage FortiGate units.

- *FortiManager CLI Reference*

  This document describes how to use the FortiManager CLI and contains a reference to all FortiManager CLI commands.

- *FortiManager Installation Guide*

  This document describes how to install a FortiManager system. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures.

- *FortiManager Release Notes*

  This document describes the new features and enhancements in the FortiManager system since the last release and lists the resolved and known issues.

- *FortiManager Log Message Reference Guide*

  Available exclusively from the Fortinet Knowledge Center, the FortiManager Log Message Reference Guide describes the structure of FortiManager log messages and provides information about the log messages that are generated by the FortiManager system.

Fortinet Tools and Documentation CD

All Fortinet documentation is available from the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation, see the Fortinet Technical Documentation web site at http://docs.forticare.com.

Fortinet Knowledge Base

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at http://kb.fortinet.com.

Comments on Fortinet technical documentation

Please send information about errors or omissions in this document or any Fortinet technical documentation to techdoc@fortinet.com.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at http://support.fortinet.com to learn about the technical support services that Fortinet provides.

Web-based manager

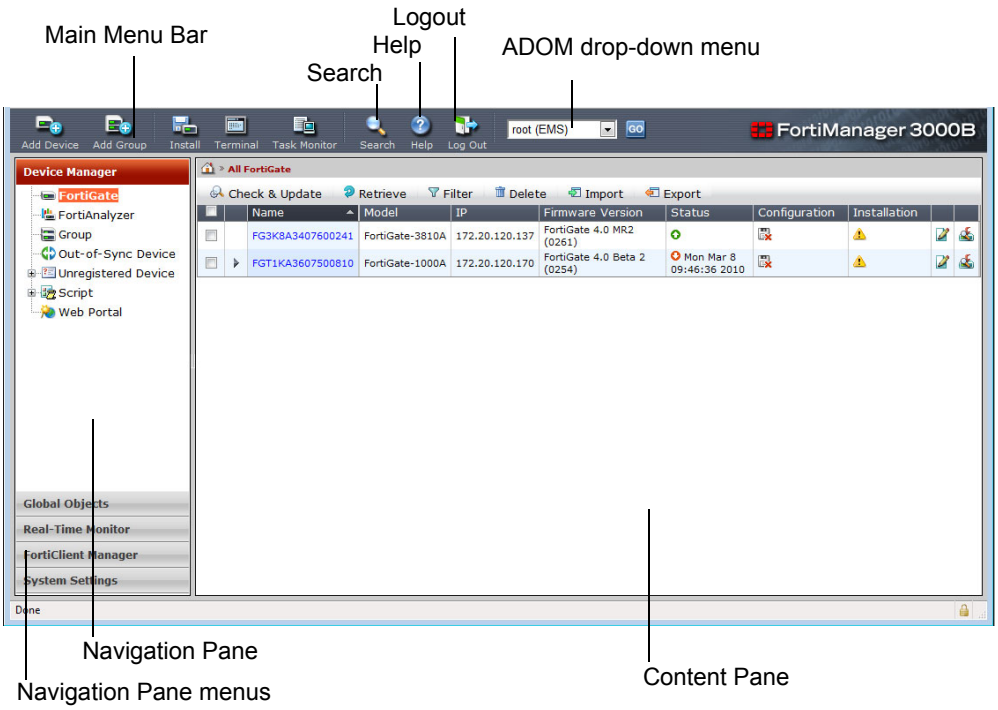
This section describes the features of the web-based manager administrative interface of your FortiManager unit.

Using HTTP or a secure HTTPS connection from any management computer using a web browser, you can connect to the FortiManager web-based manager to configure and manage the FortiManager system. The recommended minimum screen resolution for the management computer is 1280 by 1024.

You can configure the FortiManager system for HTTP and HTTPS web-based administration from any FortiManager interface. To connect to the web-based manager you require a FortiManager administrator account and password. The web-based manager supports multiple languages, but by default appears in English on first use.

Use the FortiManager command line interface (CLI) to configure many of the same FortiManager settings that you can configure from the web-based manager, as well as additional CLI-only settings. The system dashboard provides an easy entry point to the CLI console that you can use without exiting the web-based manager by selecting the *Terminal* button on the Main Menu Bar.

Figure 2: Default FortiManager Configuration window (EMS)



The illustration above shows the FortiManager web-based manager in Element Management mode (EMS). When in Global Management mode (GMS), the web-based manager is similar, however, due to the nature of the Global Management mode, there are minor differences in the Navigation Pane menus and options. For more information on these two modes see “Administrative domain modes” on page 34.

The three main parts of the FortiManager web-based interface are the Main Menu Bar, the Navigation Pane, and the Content Pane. Use the web-based manager menus, lists, and configuration pages to configure most FortiManager settings. Configuration changes made using the web-based manager take effect immediately without resetting the FortiManager system or interrupting service.

The web-based manager also includes detailed online help. Selecting *Help* on the Main Menu Bar displays help for the current web-based manager module.

Main Menu Bar

The Main Menu Bar provides buttons for quick access to commonly used features. The default Main Menu Bar includes Device Manager buttons. See "Main menu Bar" on page 82. The Main Menu Bar includes different buttons in the detached Security Console window, and in FortiClient Manager. See "Detach Security Console" on page 198, and "Main Menu Bar" on page 304 respectively.

Buttons on the Main Menu Bar allow you to perform the following system tasks:

- Search allows you to search for information in global objects. See "Searching for global objects" on page 106.
- Help allows you to access the online help for the section of the FortiManager system you are currently using.
- Log Out allows you to exit the FortiManager system web-based interface. See "Connecting to the web-based manager" on page 27.

The ADOM drop-down menu allows easy switching between ADOMs or performing ADOM management and editing. This menu is only available to the `admin` administrator. Other administrator accounts can access only one ADOM, and the name of that ADOM along with one of EMS or GMS for the management mode will be displayed. See "Assigning administrators to an ADOM" on page 38.

This display is also what appears when you log in as the admin administrator. Administrators with non-`admin` access will see fewer buttons on the Main Menu Bar.

Go to *System Settings* > *General* > *Dashboard* to view detailed information about the status of your FortiManager system on the system dashboard. The dashboard displays information such as the current firmware version, number of connected devices, connected interfaces, and system resources. It also shows if the FortiManager system is connected to a FortiAnalyzer unit.

Navigation Pane

In the Navigation Pane, on the left of the interface display, you can select and view the configuration options for devices and groups (Device Manager), and the FortiManager system itself (System Settings). You can also see configuration options for objects to be used in device configurations (Global Object and Security Console), and display various information about devices in real time (Realtime Monitor).

The items listed in the Navigation Pane vary based on if you are in EMS or GMS mode. This guide notes differences where they occur. For a list of differences between EMS and GMS mode, see "Administrative domain mode feature comparison" on page 35.

Content Pane

When you select an item in the Navigation Pane, the information is displayed in the Content Pane. This includes lists of devices or objects, screens to create or edit devices or obejcts, and other configuration related tasks. The Content Pane features a menu bar at the top, in addition to the Main Menu Bar. The Content Pane menu bar includes buttons to perform basic tasks such as create, edit, delete, and search. The options on the menu can change depending on what task you are performing, and what infomration is being displayed.

Connecting to the web-based manager

To connect to the web-based manager, you require:

- a FortiManager system connected to your network according to the instructions in the QuickStart Guide and Install Guide for your FortiManager system
- the IP address of a FortiManager interface that you can connect to
- a computer with an Ethernet connection to a network that can connect to the FortiManager system
- a supported web browser such as Firefox, Internet Explorer, or Safari with Javascript enabled.

To connect to the web-based manager

1. Start your web browser and browse to https:// followed by the IP address of the FortiManager system interface that you can connect to.

   For example, if the IP address is 192.168.1.99, browse to https://192.168.1.99. (remember to include the “s” in https://).

   To support a secure HTTPS authentication method, the FortiManager system ships with a self-signed security certificate, which is offered to remote clients whenever they initiate a HTTPS connection to the FortiManager system. When you connect, the FortiManager system displays two security warnings in a browser.

   The first warning prompts you to accept and optionally install the FortiManager system’s self-signed security certificate. If you do not accept the certificate, the FortiManager system refuses the connection. If you accept the certificate, the FortiManager login page appears. The credentials entered are encrypted before they are sent to the FortiManager system. If you choose to accept the certificate permanently, the warning is not displayed again.

   Just before the FortiManager login page is displayed, a second warning informs you that the FortiManager certificate distinguished name differs from the original request. This warning occurs because the FortiManager system redirects the connection. This is an informational message. Select OK to continue logging in.
2. Type `admin` or the name of a configured administrator in the *Name* field.
3. Type the password for the administrator account in the *Password* field.
4. Select *Login*.

Changing the web-based manager language

You can change the web-based manager to display language in English, Simplified Chinese, Traditional Chinese, or Japanese. For best results, you should select the language that the management computer operating system uses. You can also set the FortiManager web-based manager to auto detect the system language and by default show the screens in the proper language, if available.

To change the web-based manager language

1 Go to *System Settings* > *Administration* > *Admin Settings*.

2 For *Web Administration*, select the web-based manager display language.

3 Select *OK*.

Changing administrative access to your FortiManager system

Through administrative access an administrator can 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.

You can change administrative access by:

- enabling or disabling administrative access from any FortiManager interface
- enabling or disabling securing HTTPS administrative access to the web-based manager (recommended)
- enabling or disabling HTTP administrative access to the web-based manager (not recommended)
- enabling or disabling secure SSH administrative access to the CLI (recommended)
- enabling or disabling SSH or Telnet administrative access to the CLI (not recommended).

To change administrative access to your FortiManager system

1 Go to *System Settings* > *Network* > *Interface*.

2 Select an interface for which to change administrative access.

3 Select one or more *Administrative Access* types for the interface.

4 Select *OK*.

Changing the web-based manager idle timeout

By default, the web-based manager disconnects administrative sessions if no activity takes place for 5 minutes. This idle timeout is recommended to prevent someone from using the web-based manager from a PC that is logged into the web-based manager and then left unattended. However, you can use the following steps to change this idle timeout.

To change the web-based manager idle timeout

1 Go to *System Settings* > *Administration* > *Admin Settings*.

2 Change the *Idle Timeout* minutes as required.

3 Select *OK*.

Connecting to the FortiManager CLI from the web-based manager

You can connect to the FortiManager CLI from the web-based manager dashboard. You can use the CLI to configure all configuration options available from the web-based manager. Some configuration options are available only from the CLI. As well, you can use the CLI to enter diagnose commands and perform other advanced operations that are not available from the web-based manager. For more information about the FortiManager CLI see the *FortiManager CLI Reference*.

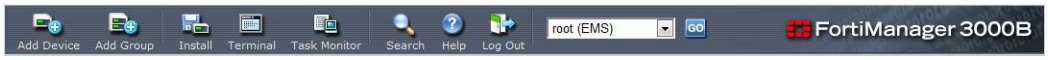
To connect to the FortiManager CLI, go to the Main Menu Bar and select Terminal. A terminal window will open allowing you to select the IP address for the connection, selecting Telnet or SSH as the connection protocol, and a Connection button to initiate the CLI session.

Note: To connect to the CLI using the above step, the FortiManager Administrative Domain mode must be set to Element Management (EMS) mode.

Main Menu Bar

At the top of the FortiManager system display is the Main Menu Bar. It includes icons for many common tasks, and ADOM navigation. Also the model of your FortiManager system is displayed on the right side of the Main Menu Bar

Figure 3: Main Menu Bar



Add Device	Select to add a FortiGate, FortiAnalyzer, or FortiMail unit to the current administration domain. See "Adding a device" on page 84.
Add Group	Select to add a group of FortiGate devices to the current administration domain. See "Adding FortiGate groups" on page 95
Install	Select to install changes from the FortiManager database to the physical devices. Optionally install to FortiGate or FortiCarrier units. See "Installing Device Configurations" on page 277. Optionally select to perform Security Domain activities such as copy, install, or review policies. See "Security Console window" on page 197.
Terminal	Select to open a terminal connection to a device. For more information on FortiManager system CLI connections, see "Connecting to the FortiManager CLI from the web-based manager" on page 28. For more information on connecting to managed devices, see "Using the CLI console for managed devices" on page 104.
Task Monitor	Select to view current or past tasks the FortiManager system is performing or has performed grouped by status. See "Using the task monitor" on page 104.
Search	Select to search for information in global objects. See "Searching for global objects" on page 106.
Help	Select to view the online help for the current display.
Log Out	Select to log out of the FortiManager web-based manager.
ADOM drop-down menu	Select an administrative domain activate. Optionally select Manage ADOMs to create, edit, or delete administrative domains. See "Administrative Domains" on page 33.
GO	Select to activate your selection in the ADOM drop-down menu.

Navigation Pane menus

The Navigation Pane menus, located on the left-hand side of the web-based manager, provide the menus for configuring and maintaining the FortiManager system and other devices such as FortiGate units, FortiMail units, and so on. Each menu in the pane is broken down into specific tasks, for easy navigation and managing of your network.

There are two operating modes (administrative domains) for FortiManager system administrators When using the FortiManager system in Global Management mode (GMS), the Navigation Pane includes an additional menu choice for Security Console which enables administrators to configure security elements common to multiple FortiGate units in a central location. Once configured, administrators can push these elements the managed FortiGate units.

When using the FortiManager system in EMS mode, the Global Objects menu choice also includes a Policies Objects option. Global Objects is the FortiManager global database where you can configure global objects and copy the configurations to the FortiManager device database for a selected device or a group of devices. For information on administrative domains and their difference, see "Administrative Domains" on page 33.

Device Manager

The *Device Manager* is where you add and manage devices through the FortiManager system. The *Device Manager* menu enables you to view the device information and status, create and manage device groups and manage firewall global policy objects. Global objects are elements of a firewall policy that are common to all FortiGate devices, such as antivirus profiles, web filters and schedules.

The *Device Manager* also is where you configure the web portal configurations, users and groups. The web portal is only available in Element Management mode (EMS).

For more information on the *Device Manager* and managing devices see the chapter "Managing Devices" on page 81.

Security Console

The *Security Console* is only available when the administrative domain mode is set to Global Management mode (GMS). Similar to the function of *Device Manager*, *Security Console* contains additional modules, such as the *VPN Console*, *Policy Console*, and *Dynamic Objects*. Because of the nature of Global Management mode, the *Security Console* enables you to configure firewall policies, VPN connections and other common FortiGate configurations that, in a corporate or MMS device management style, you can push to all devices to have a common configuration.

For more information on using the *Security Console*, see the chapter "Security Console" on page 197.

Real-Time Monitor

The *Real-Time Monitor* enables you watch your FortiGate devices for trends, outages, or events that require attention. Where you would normally log on to each individual FortiGate unit to view system resources and information, you can view that same information for all your FortiGate devices in the *Real-Time Monitor*.

In the *Real-Time Monitor*, all actions and configurations are by device. The FortiManager system reads all of its information from the FortiGate devices from SNMP traps and variables. SNMP traps and variables provide access to a wide array of hardware information from percent of disk usage to an IP address change warning to the number of network connections. SNMP must be properly configured on both the FortiGate units and your FortiManager system for this information to stored and collated.

For more information on using the *Real-Time Monitor*, see the chapter "Real-Time Monitor" on page 283.

FortiClient Manager

The *FortiClient Manager* is only available when the administrative domain mode is set to Element Management mode (EMS).

The *FortiClient Manager* enables you to centrally manage FortiClient software running on client computers throughout the organization. With this menu option, you can configure global options such as web filters, user groups and license keys which you can then push to the corporation, rather than one installation at a time. The FortiClient Manager also enables you to monitor FortiClient installations to see if any virus or firewall alerts are occurring so you can quickly react to any evolving issues.

For more information on using the *FortiClient Manager*, see the chapter "FortiClient Manager" on page 303.

System Settings

System Settings enables you to configure and maintain the basic system settings of the FortiManager system. It is like the central management of the device to make it operational and to connect it to the network, including network configurations, and adding and maintaining administrators and their access privileges. You can also configure the FortiManager logging, FortiGuard options and firmware monitoring.

For more information on configuring the system settings see the chapter "System Settings" on page 41.

Administrative Domains

FortiManager administrative domains enable the admin administrator to create groupings of devices for configured administrators to monitor and manage.

FortiManager can manage a large number of Fortinet devices. This enables administrators to maintain managed devices specific to their geographic location or business division. This also includes FortiGate units with multiple configured VDOMs.

Each administrator is tied to an administrative domain (ADOM). When that particular administrator logs in, they see only those devices or VDOMs configured for that administrator and ADOM. The one exception is the admin administrator account which can see and maintain all administrative domains and the devices within those domains.

In earlier versions of FortiManager, individual devices were assigned to administrator profiles. In FortiManager 4.0, you assign devices to an administrative domain (ADOM) and each administrator is assigned an administrative domain.

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

The maximum number of administrative domains you can add depends on the FortiManager system model. The table below outlines these limits.

FortiManager Model	Maximum ADOMs
100	2
100C, 400A, and 400B	10
1000B	25
1000C	50
3000 and 3000B	100
3000C	200
5001A	100

This section includes the following topics:

Administrative domain modes

Administrative domains have two modes of operation. When you create a new administrative domain, you select the mode best suited for the administration of the devices in that domain. The available modes are Elemental Management System (EMS) and Global Management System (GMS). Depending on the mode selected, there are slight variances to the feature set available within the web-based manager. These variances do not necessarily restrict an administrator from managing their devices. Each mode has unique capabilities to compliment their roles.

Note: A device can only be managed in one mode. For example you cannot have a FortiGate unit managed by two administrators in two different modes. Due to the differences in each mode, outlined below, this can not be an option.

The default operating mode for the FortiManager system is Element Management System. The `admin` administrator, by default, always logs into the `root` administrative domain, which is always in Element Management mode. The admin administrator can switch to Global Management mode if required. See "Switching between administrative domains" on page 39.

By default, administrator accounts other than the `admin` account are assigned to the `root` administrative domain, which includes all devices in the device list. By creating administrative domains that contain a subset of devices in the device list, and assigning them to administrator accounts, you can restrict other administrator accounts to a subset of the FortiManager system's total devices or VDOMs.

Note: The `admin` administrator account cannot be restricted to a single administrative domain.

Elemental Management System

Element Management System (EMS) mode enables administrators to manage multiple devices with multiple or varying configurations. Administrators may have many FortiGate units or VDOMs, and each unit or VDOM requires a unique or specific configuration, firewall policies, user groups, VPN configurations and so on. EMS mode allows you to select the elements of a configuration that are common to multiple units or VDOMs, and use those elements to help configure those units.

Element Management mode provides a number of features that are not available in GMS mode. This does not limit one mode over another, but provides a different feature set for managing devices. Element Management mode is useful for managing units with very different configurations.

Element Management mode includes:

- administrative web portal configurations
- XML API support
- Script Manager
- the option to access ADOMs from *System Settings* > *Administration* > *ADOM*
- no Security Console.

Global Management System

Global Management System (GMS) mode enables administrators to manage multiple devices with a single configuration. Administrators may have many FortiGate units or VDOMs. In a corporate environment, each firewall configuration and installation will have the same policies, groups, VPN configurations and setup. Where only parts of the units or VDOMs configuration are shared in EMS mode, in GMS mode the entire configuration is shared by the units or VDOMs.

In GMS mode administrators can create the configurations and push them to all devices in an all-at-once approach.

Note: In GMS mode, updating or changing an individual device is not an option. Any update or change will affect all devices being managed.

Global Management mode provides a number of features that are not available in EMS mode. This does not limit one mode over another, but provides a different feature set for managing devices. Global Management mode is useful when you need to ensure all units are configured the same way, with the same level of security such as to satisfy security audits.

Global Management mode includes Security Console management for global elements including VPN, dynamic objects and policy console. Global Management mode does not include the administrative web portal configurations, or the XML API.

Administrative domain mode feature comparison

To summarize the FortiManager administrative domain modes and what features are available, see the table below.

Features included	EMS mode	GMS mode
Web Portal	Yes	-
Script Manager	Yes	-
Security Console	-	Yes
XML API	Yes	-
FortiGuard Center	Yes	-
ADOM management	through Main Menu Bar or System Settings	only through Main Menu Bar

Administrative domain device modes

An administrative domain has two device modes: normal and advanced. In normal mode, you cannot assign different FortiGate VDOMs to multiple FortiManager administrative domains. The FortiGate unit can only be added to a single administrative domain.

In advanced mode, you can assign different VDOMs from the same FortiGate unit to multiple administrative domains.

To change to a different device mode, use the following command in the CLI:

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

Normal mode is the default. To change from advanced back to normal, you must ensure no FortiGate VDOMs are assigned to an administrative domain.

Enabling administrative domains

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

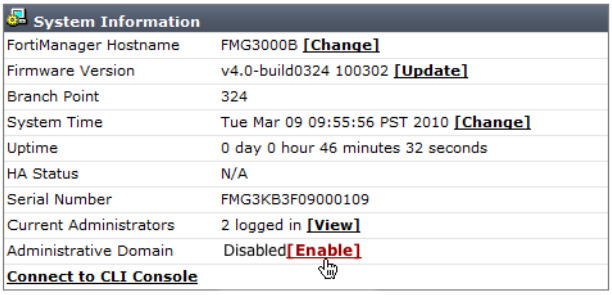
To enable administrative domains

1 Log in as `admin`.

2 Go to *System Settings* > *General* > *Dashboard.*

3 In *System Information*, select *Enable* next to *Administrative Domain*

Figure 4: Enabling administrative domains



Once enabled, the Main Menu Bar will have a new ADOM drop down menu which provides you access to the administrative domains so you can move between ADOMs as well as add, edit and remove ADOMs.

Disabling administrative domains

Once you add administrative domains to the FortiManager system, you will notice that the Disable option for *Administrative Domains* does not appear. Administrative domains cannot be disabled if administrative domains are still configured and listed and they still have devices managed within it.

To remove the administrative domains

1 Remove the managed devices from all administrative domains.

- Switch to the administrative domain by selecting the *ADOM* from the ADOM drop-down menu on the Main Menu Bar. For more information see “Switching between administrative domains” on page 39.
- Select the checkboxes for each device and select *Delete*.

2 Delete all non-root administrative domains

- Select *Manage ADOMs* from the ADOM drop-down menu on the Main Menu Bar.
- Select the checkbox beside the ADOMs and select *Delete*.

After removing the ADOMs, you can now disable the administrative domain feature.

To disable administrative domains

1 Go to *System Settings* > *General* > *Dashboard.*

2 In *System Information*, select *Disable* next to *Administrative Domain.*

Adding an administrative domain

To add an administrative domain, you must be logged in as the `admin` administrator. You must also first enable administrative domains in the web-based manager.

To enable administrative domains, go to *System Settings* > *General* > *Dashboard, and select Enable for Administrative Domain.*

To add an administrative domain

1 Go to System *Settings* > *Administration* > *ADOM*.

Alternatively, select *ADOM* from the Main Menu Bar.

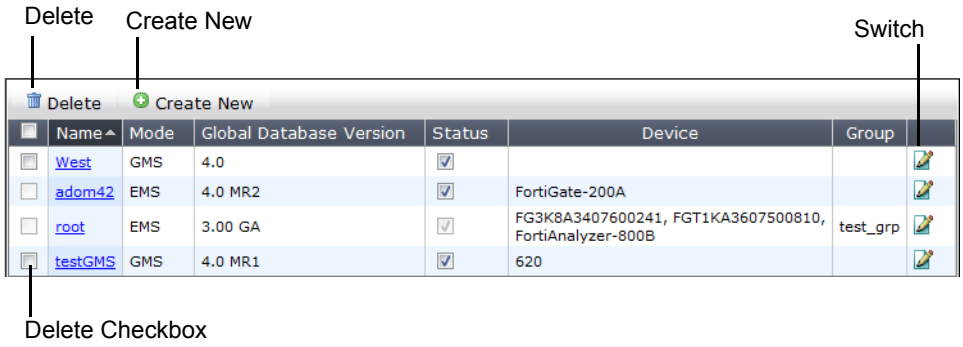
2 Enter the following information and select *OK*.

Name	Enter a name for the administrative domain.
Mode	Select either *EMS* or *GMS* mode. For more information on what the features are for each mode before selecting, see "Administrative domain modes" on page 34.
Global Database Version	Select the minimum firmware release for the global database.
Migration Mode	Select to enable migration options. When upgrading FortiGate units to a new OS revision, if attributes of global objects change from one FortiOS version to the next, the global object will contain both versions of the object. This feature is ideal for firmware migration. Whenever upgrading the FortiManager system, the global object definitions include any new changes made to the database structure. The FortiGate administrator needs to adjust the global objects as needed. If no changes are made, the default values for the object are stored and used.
Enable	Select to enable the administrative domain. When unselected, administrators configured for the administrative domain will not be able to log into the FortiManager system. If you choose to not enable the administrative domain, you can enable it later, by going to the ADOM by selecting *ADOM* from the Main Menu Bar and selecting the ADOMs check box in the *Status* column.

The administrative domain window

When an administrative domain is added, the FortiManager system adds the information to the administrative domain table.

Figure 5: Administrative domain table



Delete checkbox	Select the check box when you want to remove one or more administrative domains. Select Delete (located above the table) to remove the domain or domains. Note that all devices must be removed from the administrative domains before you can delete the domains.
Create New	Select to create a new administrative domain. See “Adding an administrative domain” on page 37.
Name	The name of the administrative domain. Select the name to enter that ADOM. The new domain information will be displayed in the Main Menu Bar.
Mode	The mode for the administrative domain. One of EMS or GMS. Once the domain has been created, the mode cannot be changed. For more information on the mode types, see “Administrative domain modes” on page 34.
Global Database Version	The global database version and release of the objects to configure for the devices.
Status	Enable or disable the administrative domain by selecting the check box for the particular domain.
Device	A list of devices in the administrative domain.
Group	A list of groups of devices in the administrative domain.
Edit	Select to make changes to this administrative domain. You can change the Global Database Version, Migration Mode, or devices assigned to this domain.

Assigning devices to an administrative domain

The admin administrator selects the devices that are in an administrative domain. You cannot assign the same device to two different domain modes. For a description of the differences, see “Administrative domain modes” on page 34.

To assign devices to an administrative domain

1. In the Main Menu Bar, select Manage ADOMs from the ADOM drop-down menu and select *GO*.
2. Select *Edit* for the domain
3. Select which devices to associate with the administrative domain from *Available member*, and select the *Right arrow* to move them to *Selected member*.

   If you have the administrative device mode set to Advanced, you can add separate FortiGate VDOMs to the administrative domain as well as FortiGate units. For more information see “Administrative domain device modes” on page 35.
4. Select *OK*.

Tip: You can move multiple devices at once. To select multiple devices, select the first device, then hold the Shift key while selecting the last device in a continuous range, or hold the Ctrl key while selecting each additional device.

Assigning administrators to an ADOM

The `admin` administrator can create other administrators and assign an administrative domain to their account, constraining them to configurations and data that apply only to devices in their administrative domain.

Note: By default, when administrative domains 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 administrative domains, see "Assigning devices to an administrative domain" on page 38.

To assign an administrator to an ADOM

1 Log in as `admin`.

Other administrators cannot configure administrator accounts when administrative domains are enabled.

2 Go to *System Settings* > *Administration* > *Administrator*.

3 Configure the administrator account, and select the *Admin Domain* that administrator account will use to access the FortiManager system.

Note: Do not select *Edit* for the `admin` account. The `admin` administrator account cannot be restricted to an administrative domain.

Switching between administrative domains

As an admin administrator, you are able to move between the various administrative domains created on the FortiManager system. This enables you to view and administer the various domains. When you log into the FortiManager system as the `admin` administrator, by default you log in to the root administrative domain in EMS mode.

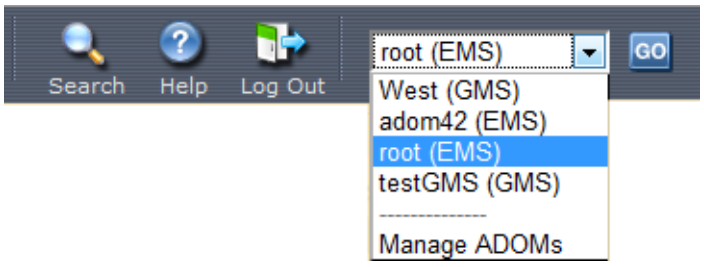
To switch to a different administrative domain

1 In the Main Menu Bar go to the ADOM drop-down menu.

2 From the drop-down menu, select the ADOM you want to enter.

3 Select *GO*.

Figure 6: Switching between domains



- Once switched over to the new administrative domain, the FortiManager system presents you with the device list for that domain. If the domain is running in Global Management mode (GMS), you will also have an additional menu selection on the left for the Security Console, for additional policy configuration. For more information on the Security Console, see "Security Console" on page 197.

System Settings

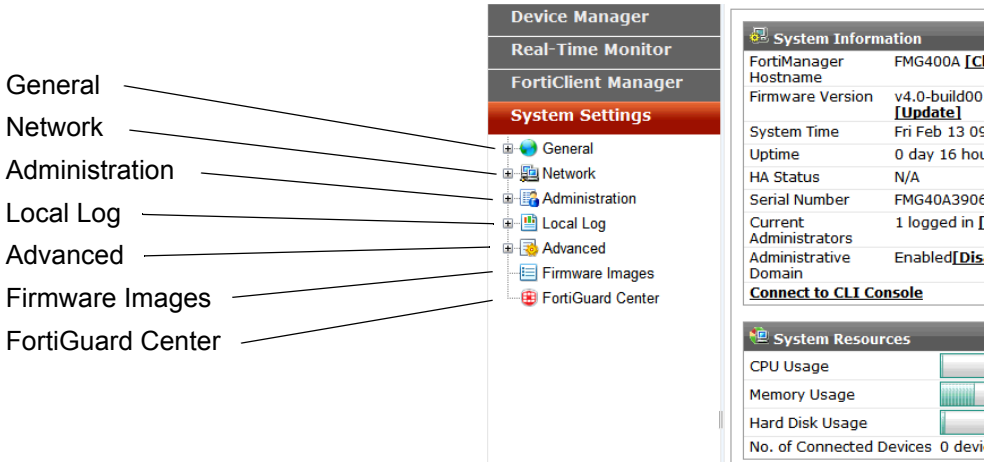
The System Settings module provides a means to manage and configure the basic system options for the FortiManager unit. This includes the basic network settings to connect the device to the corporate network, the configuration of administrators and their access privileges, managing and updating firmware for the device and configuring logging and access to the FortiGuard center for updates.

F

Note: If the administrator account you logged on with does not have System module privileges, 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 profile” on page 63.

The System Settings option in the sidebar contains seven category selections:

Figure 7: System Settings options



General	The General settings are where you configure and monitor the main system information. Options include: • **Dashboard** for monitoring the system status and performing general configuration such as setting time and uploading new firmware for the FortiManager unit. • **Backup and Restore** to save a copy of the system configuration and restore at a later time should something fail on the FortiManager system. It is always a good idea to back up the configuration when any changes are made to ensure you have the latest configuration stored. • **Firmware Update** to upgrade or downgrade the firmware image of the FortiManager operating system. • **Diagnose Tools** to configure a ping server and Traceroute address. • **Certificates** to add authorization certificates for administrators. • **HA** to configure high-availability load balancing or redundancy between multiple FortiManager units to ensure no single point of failure for network management. • **SNMP** to configure FortiGate and FortiManager reporting through SNMP traps. • **RAID** to configure RAID levels on FortiManager units with multiple hard disks, to ensure data security and recovery in event of a disk failure. For more information see "General settings" on page 42.
Network	Enables you to configure FortiManager network interfaces, routing, and DNS settings. For more information, see "Network settings" on page 59.
Administration	Enables you perform administrative tasks as well as maintain the administrative users connecting to the FortiManager unit. Options include: • **ADOM** for setting up, configuring and maintaining administrative domains. • **Administrator** to add new administrative users. • **Profile** to set up access levels for the administrative users. • **Logged-in Session** to monitor which administrators are logged into the FortiManager unit, their location (IP address) and how long before their idle time expires. It also enables you to disconnect the user if needed. • **RADIUS/LDAP Server** to connect to a corporate authorization server for administrative log in. • **Admin Settings** to configure connection options for the administrator including port number, language of the web-based manager and idle timeout. For more information, see "Configuring administration settings" on page 61.
Local Log	Enables you to configure the types of log messages the FortiManager unit records and where the logs are stored. This option also enables you to view local log messages to monitor the status of the FortiManager unit on the network. For more information, see "Local log settings" on page 71.
Advanced	Enables you to configure metadata fields for FortiGate objects, and configure chassis management configuration for FortiGate-5000 series shelf managers. For more information, see "Advanced Metadata" on page 76.
Firmware Images	Enables you to view the available firmware images for managed devices, and download firmware images for loading onto the managed devices. For more information see "Downloading firmware images" on page 274.
FortiGuard Center	Displays the version and status of antivirus, IPS and antispam versions, and enables you to configure override servers and push update settings. For more information see "Overriding default IP addresses and ports" on page 258.

General settings

The General settings are where you configure and monitor the system information of the FortiManager unit.

Go to *System Settings* > *General* to view the General options. There you select one of these options:

- Dashboard

- Backup and Restore
- Firmware Update
- Diagnostic Tools
- Certificates
- High Availability
- SNMP
- RAID (on FortiManager systems that have multiple hard disks)

Dashboard

Go to *System Status* > *General* > *Dashboard* to view detailed information about the status of your FortiManager unit on the system dashboard. The dashboard displays information such as the current firmware version, license information of managed devices, alert message information, connected interfaces, and system resources. It also shows whether the FortiManager unit is connected to a FortiAnalyzer unit.

Demo mode

FortiManager includes a demo mode option, available on the Dashboard. Demo mode enables you to see how the FortiManager monitors FortiGate devices, and how the web portal operates. This provides an easy way to demonstrate the capabilities of the FortiManager unit to company officials, or customers for managing their FortiGate network protection systems.

The demo comes pre-configured with and Administrative Domain in Element Management mode, configured with a FortiGate-5001A blade with 10 VDOMS, and three FortiGate-50B devices. The demo mode is otherwise is a fully functional version of the FortiManager operating system; you can add users, configure various aspects of the devices, so you can see how managing FortiGate devices works.

Note that the administrative domain operates in an “offline mode”, and the FortiManager unit will not setup a FortiGate-FortiManager tunnel or communicate with other devices.

Figure 8: Demo mode dashboard widget

To enable demo mode

1 Go to *System Settings* > *General* > *Dashboard*.

2 In the *Demo Information* widget, select *Enable*.

Once enabled, you can either run the FortiManager unit in demo mode or try the demo of the web portal.

Figure 9: Demo mode enabled

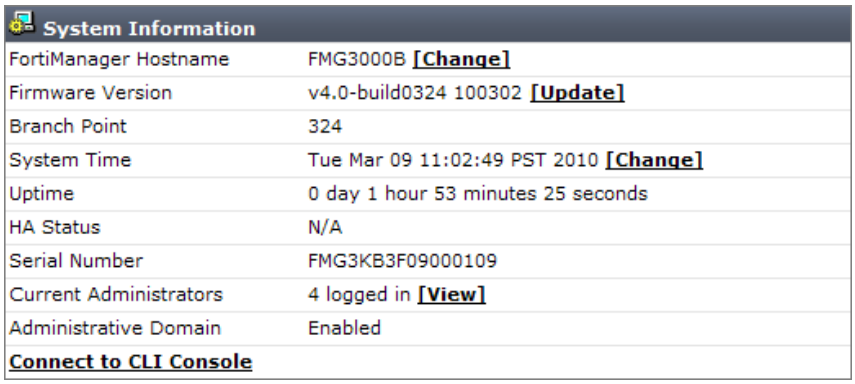
There are two possible ways to log in to the demo mode once it is enabled. You can either select the *Login to Demo* button on the widget, or when logging into the FortiManager, select the *Log in to Demo Mode* check box and select *Login*. No other user name or password is required.

To log out of demo mode, simply select the Logout arrow in the upper-right corner of the web-based manager as you would any other time you logged out as the administrator.

System Information

The *System Information* widget displays the current status of the FortiManager unit and enables you to configure some system settings as well.

Figure 10: System Information



FortiManager Hostname	The identifying name assigned to this FortiManager unit. To change the host name, select *Change* and enter a new name for the FortiManager unit, up to 35 characters.
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 Support web site at http://support.fortinet.com. Select *Update* and select the firmware image to load from the local hard disk or network volume.
Branch Point	Software build number
System time	The current time on the FortiManager internal clock. To change the time, select *Change*. For more information, see “To set the system time” on page 45.
Uptime	The duration of time the FortiManager unit has been running since it was last started or restarted.
HA Mode	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 “FortiManager HA” on page 383.
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.
Current Administrators	The number of administrators that are logged in. To view the list of administrators, select *View*. For more information, see “To view the current administrators” on page 45.
Administrative Domain	Displays whether Administrative Domains are enabled. For more information, see “Administrative domain modes” on page 34
Connect to CLI Console	Select to open a command line interface (CLI) window to configure the FortiManager unit with the CLI.

Configuring basic system settings

In the *System Information* widget on the Dashboard, there are several shortcuts that allow you to:

- Update the firmware from your local machine
- Update the firmware from the Device Manager Firmware tab
- View the administrators currently connected
- Configure the host name
- Change the system time.

To update the firmware image (local)

1. Download the new firmware image for your FortiManager unit from the Support web site at http://support.fortinet.com to your local machine.
2. Select *System Settings* > *General* > *Dashboard* and under *Firmware version* select *Update*.
3. In the new window, browse to the firmware located on your local machine and select *OK*.

To view the current administrators

1. Select *System Settings* > *Administration* > *Administrator*.
2. In the new window, you can view, delete, or modify the session information.

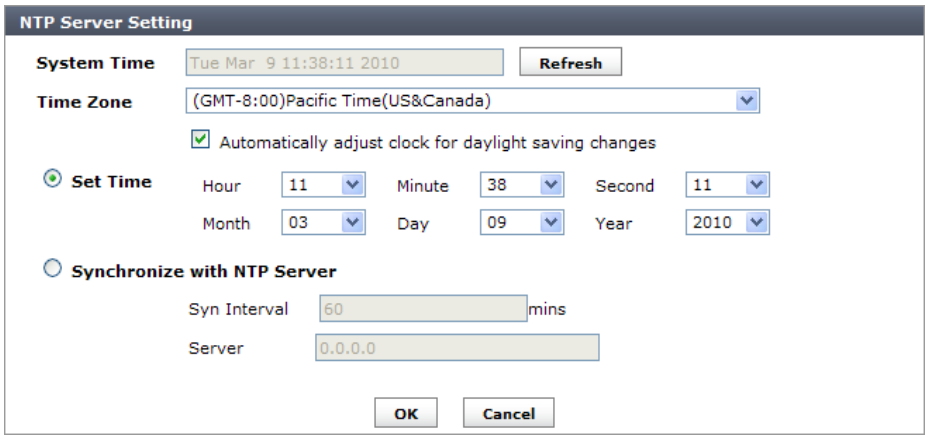
To configure the hostname

1. Go to *System Settings* > *General* > *Dashboard*.
2. Select *Change* next to *FortiManager Hostname*.
3. Enter a new name for the FortiManager unit, up to 35 characters.

To set the system time

1. Go to *System Settings* > *General* > *Dashboard*.
2. Select *Change* next to *System Time.*

Figure 11: System time settings



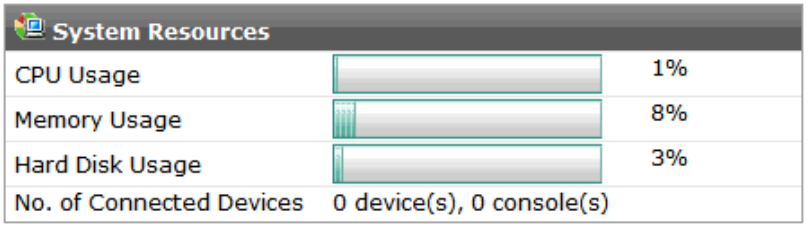
System Time	The current FortiManager unit date and time.
Refresh	Select to update the display of the current system date and time.

Time Zone	Select the FortiManager unit time zone. This is required even if you use an NTP server to set the time.
Automatically adjust clock for daylight savings changes	Select to automatically adjust clock for daylight savings time.
Set Time	Select to set the date and time manually. Enter the values for the *Year*, *Month*, *Day*, *Hour*, *Minute*, and *Second* fields.
Synchronize with NTP Server	Select to use an Network Time Protocol (NTP) server to automatically set the system date and time. You must specify the server and synchronization interval.
Syn Interval	Specify how often the FortiManager unit synchronizes with the NTP server in minutes. For example, a setting of 1440 minutes causes the unit to synchronize its time once a day.
Server	Enter the IP address or DNS resolvable domain name of an NTP server. To find an NTP server go to http://www.ntp.org.

System Resources

The *System Resources* widget on the Dashboard displays the usage status of the CPU, memory and hard disk. It also provides a visual reference to the number of connected devices to the FortiManager unit.

Figure 12: System Resource information



CPU Usage	The current CPU utilization. The web-based manager displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.
Memory Usage	The current memory utilization. The web-based manager displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.
Hard Disk Usage	The current hard disk (local disk) utilization. The web-based manager displays hard disk usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.

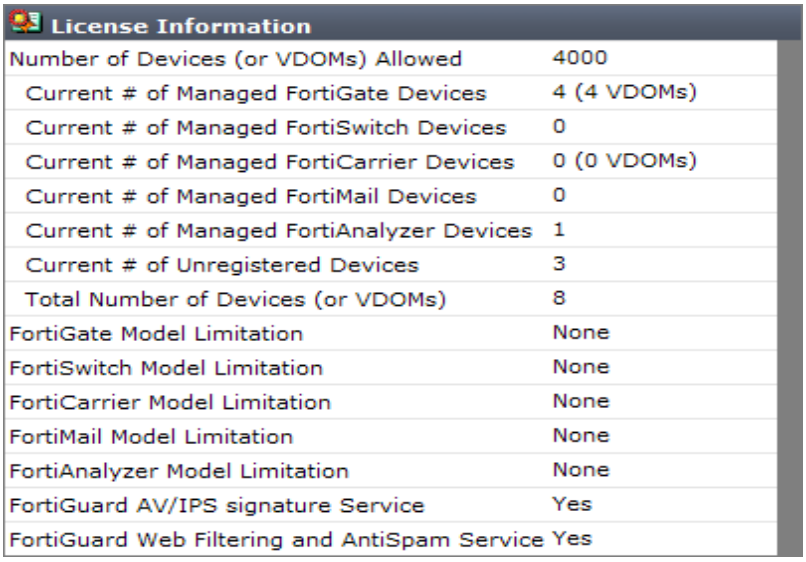
You can refresh the information displayed in the System Resources widget by selecting *Refresh Now*, or setting the *Automatic Refresh Interval*, both found at the bottom of the Dashboard window.

License Information

The license information displayed on the dashboard shows, in a single snapshot, the devices being managed by the FortiManager unit and the maximum numbers of devices allowed. The maximums are based on FortiManager system resources.

An important listing is the number of unregistered devices. These are devices not registered by the administrator with Fortinet. If the device is not registered, it cannot be updated with new antivirus or IPS signatures or provide antispam services either from FortiGuard services directly or from the FortiManager updates.

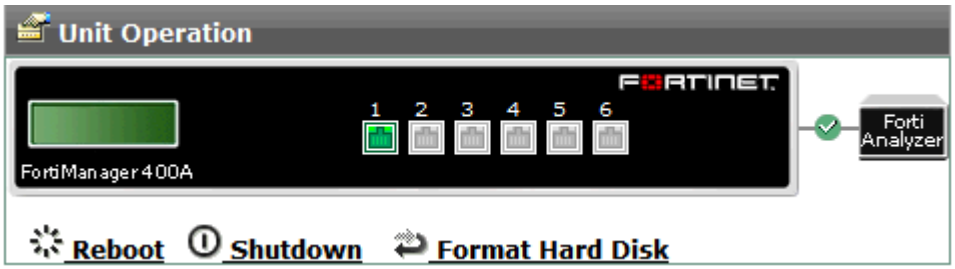
Figure 13: License Information



Unit Operation

The *Unit Operation* widget on the Dashboard is a graphic representation of the FortiManager unit. This graphic displays status and connection information for the ports of the FortiManager unit. It also enables you to shutdown, restart and format the FortiManager hard disk, with a quick click of the mouse.

Figure 14: FortiAnalyzer connection status



Port numbers (vary depending on model)	The image below the port name indicates its status by its color. Green indicates the port is connected. Grey indicates there is no connection. For more information about a port's configuration and throughput, position your mouse over the icon for that port. You will see the full name of the interface, the IP address and netmask, the status of the link, the speed of the interface, and the number of sent and received packets.
FortiAnalyzer	The icon on the link between the FortiManager unit graphic and the FortiAnalyzer graphic indicates the status of their connection. An 'X' on a red circle indicates there is no connection. A check mark on a green circle indicates there is communication between the two units. For information about configuring FortiAnalyzer logging on your FortiManager unit, see "FortiAnalyzer Devices" on page 299.
Reboot	Select to restart the FortiManager unit. You are prompted to confirm before the reboot is executed.

Shutdown	Select to shutdown the FortiManager unit. You are prompted to confirm before the shutdown is executed.
Format Hard Disk	Select to format the FortiManager internal hard disk. You are prompted to confirm before formatting. Reformatting the hard disk will wipe out all data on the disk including logs, configurations, and backups on the hard disk. Its is highly recommended you backup all data before formatting the hard disk.

Alert Message Console

The *Alert Message Console* widget on the Dashboard displays the critical alert messages for events occurring on the FortiManager unit.

For more detail on these alert messages and other recorded system information, select the **>>** icon to access local logs. For more information on logs and viewing logs, see "Log access" on page 75.

Backup and Restore

The Backup and Restore menu enables you to back up and restore your FortiManager configuration to your management PC or central management server. It is a good idea to backup the FortiManager configuration 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. It is a good idea to back up the configuration after making any changes to the configuration of the FortiManager unit or settings that affect the managed devices.

The backup and restore option enables you to do the 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.

To backup or restore the FortiManager configuration, go to *System Settings* > *General* > *Backup and Restore*.

Figure 15: Backup and Restore

Category	The type of back up or restore.
Latest Access	The date and time of the last back up or restore.
Next Scheduled	You can configure a scheduled backup to ensure that configurations are backed up in the event of a system failure or reset. This column displays the time of the next scheduled back up, if configured.
Backup	Select to immediately back up the configuration to a file. For more information, see "Backing up the configuration" on page 49.

Scheduled Backup	Select to configure scheduled back ups for that category. For more information on configuring scheduled backups, see "Scheduling backups" on page 49.
Restore	Select to restore the configuration from a file. Enter the path and filename of the file. When restoring the system configuration, the FortiManager unit restarts, loading the system configuration. You will need to reconnect to the web-based manager and review your configuration to confirm that the restored system configuration has taken effect.

Fortinet recommends backing up all configuration settings from your FortiManager unit before upgrading the FortiManager firmware.

Backing up the configuration

The following procedures enable you to back up your current configuration through the web-based manager. If your FortiManager unit is in HA mode, switch to Standalone mode.

To back up the FortiManager configuration

1 Go to *System Settings* > *General* > *Backup and Restore*.

2 Select the *Backup* icon.

3 Save the configuration file to your management computer.

Scheduling backups

Scheduling backups at a regular interval ensures that you can have a backup of the FortiManager configuration, no matter when changes are made. It also ensures you do not forget to backup the configuration.

To schedule backups of the FortiManager configuration

1 Go to *System Settings* > *General* > *Backup and Restore*.

2 Select the Scheduled Backup icon for the configuration that you want to automatically back up.

3 Select *Enable*.

4 Enter the following information about the server:

Backup Destination	Enter the IP address of the back up server.
Backup to Remote Path	Enter the path and file name on the backup server where the configuration where FortiManager saves the configuration file.
Backup Protocol	Select the file transfer protocol to use.
User Name	Enter the user name required to authenticate, on the backup server.
Password	Enter a password for the above user name.
Day	Select a day of the week or multiple days of the week when the backup file will be backed up on.
Time	Select a time when the backup file will be backed up on the day or days specified. The time is in hours and minutes.

5 Select *OK*.

System checkpoint

The system checkpoint component of the backup and restore feature of FortiManager enables you 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 to the network to when it was in working order, and not have to be concerned about which device has which versions of the firmware installed and so on. These are, in essence, snapshots of your Fortinet managed network system.

This can also be useful when installing new firmware to devices or making a major configuration change to the network. If the update or modification does not go well, it is a click away from being restored to a “good” version of the configuration when everything worked fine.

A system checkpoint backup includes:

- the current configuration file from each managed device
- the entire system configuration of the FortiManager unit.

To create a checkpoint backup

1. Go to *System Settings* > *General* > *Backup and Restore* > *System Checkpoint*.
2. Select *Create New*.
3. Enter a description, up to 63 characters, for the reason or state of the backup.
4. Select *Submit*.

Firmware Update

Firmware update enables you to upload new or older FortiManager firmware images from a management PC or from the FortiManager hard disk.

Current and past firmware images are available from the Customer Support web site at http://support.fortinet.com. You need to log into the site with the information you used to register the Fortinet devices.

Caution: Always back up your configuration before installing a patch release, upgrading/downgrading firmware, or resetting configuration to factory defaults.

Note: For information on backing up the FortiManager configuration, see “Backup and Restore” on page 48.

To upload a new firmware image

1. Go to *System Settings* > *General* > *Firmware Update*.
2. Select to upload the firmware from a local PC or server.
3. If you are upload from a local PC, select *Browse* to locate the file.
4. Select *OK*.

For more information on upgrading or downgrading the firmware, see “Managing Firmware Versions” on page 393.

Diagnostic Tools

Your FortiManager unit works by communicating with FortiGate, FortiMail, and FortiAnalyzer devices. When the communication isn’t functioning properly, you can use the diagnostic tools to help troubleshoot the problem.

Figure 16: Diagnostic tools

Ping	Enter an IP address or resolvable domain name to ping and select *Go*. If the number of packets received equals the number of packets transmitted, a working network connection exists between the FortiManager unit and the IP address tested. If you enter a domain name and the result is an 'unknown host' message, the destination cannot be contacted. Among the possible causes are: • There is no network connectivity to the destination. • The destination host is not functioning. • The destination host is not configured to respond to ping requests. • If you're entering a domain name, the FortiManager unit DNS configuration may be incorrect. For information, see "Configuring DNS" on page 61.
Traceroute	Enter an IP address or resolvable domain name to trace and select *Go*. The FortiManager unit will display the route the packets take to their destination.

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.

To create a certificate request

1 Go to *System Settings* > *General* > *Certificates* > *Local Certificates*.

2 Enter the information as required and select *Go*.

The certificate window also enables you to export certificates for authentication, importing and viewing.

High Availability

FortiManager high availability (HA) provides a solution for a key requirement of critical enterprise management and networking components: enhanced reliability. Additional FortiManager units can be configured to provide failover protection for the primary FortiManager unit.

For more information, see "FortiManager HA" on page 383

SNMP

Simple Network Management Protocol (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* > *General* > *SNMP v1/v2c* to configure your FortiManager system's SNMP settings.

The Real Time Monitor uses SNMP traps and variables to read, log, and display information from connected FortiGate devices. For more information, see "Real-Time Monitor" on page 283.

SNMP has two parts - the SNMP agent or the device that is sending traps, and the SNMP manager that monitors those traps. The Real Time Monitor is the manager that monitors the FortiGate devices that are sending traps. To this end, 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 and v2c 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.

Note: This section deals only with FortiManager system generated SNMP traps, not FortiGate unit generated traps. For information on FortiGate unit generated traps, see "Real-Time Monitor" on page 283.

The following sections provide an overview of the SNMP settings and MIB files that define the Fortinet SNMP traps and variables.

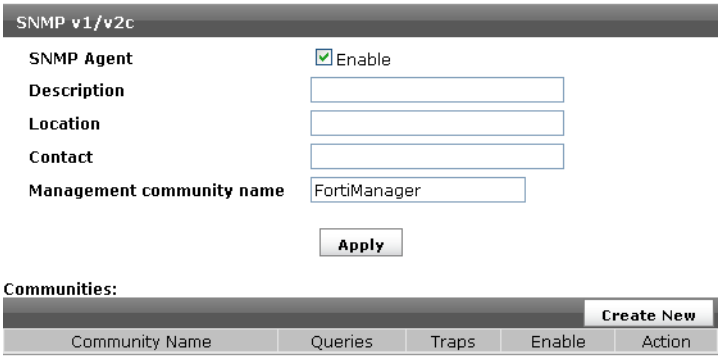
Configuring the SNMP Agent

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 ocurring. 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* > *General* > *SNMP v1/v2c* to configure the SNMP Agent.

Figure 17: SNMP configuration



SNMP Agent Select to enable the FortiManager SNMP agent. When this is enabled, it sends FortiManager SNMP traps.

Description	Enter a description of this FortiManager system to help uniquely identify this unit.
Location	Enter the location of this FortiManager system to help find it in the event it requires attention.
Contact	Enter the contact information for the person in charge of this FortiManager system.
Management Community Name	Enter the name to use for the community created by the FortiManager system during configuration of new FortiGate devices. The default value is FortiManager. This field can be a maximum of 127 characters long.
Communities	The list of SNMP communities added to the FortiManager configuration.
Create New	Select Create New to add a new SNMP community. If SNMP Agent is not selected, this control will not be visible. For more information, see "Configuring an SNMP Community" on page 53.
Community Name	The name of the SNMP community.
Queries	The status of SNMP queries for each SNMP community.
Traps	The status of SNMP traps for each SNMP community.
Enable	Select to enable or unselect to disable the SNMP community.
Delete icon	Select to remove an SNMP community.
Edit icon	Select to edit an SNMP community.

Configuring an SNMP 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.

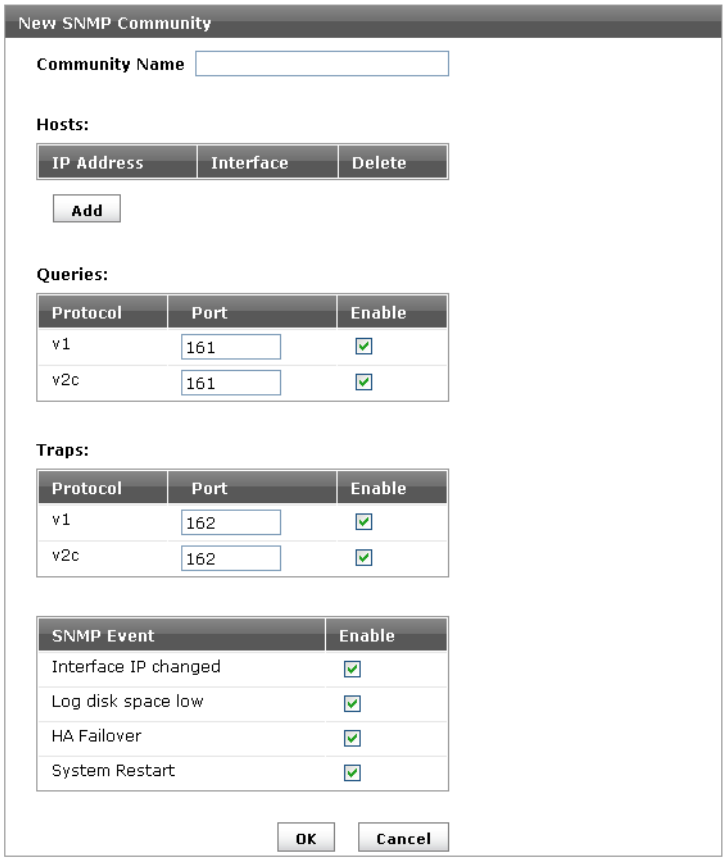
Note: These SNMP communities do not refer to the FortiGate devices the FortiManager system is managing. For more information on FortiGate device SNMP, see either "Real-Time Monitor" on page 283, or the *FortiGate Administration Guide*.

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 8 hosts to each community. Hosts can receive SNMP device traps, and information.

Select *Create New* on the SNMP v1/v2c screen to configure an 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.

Figure 18: FortiManager SNMP Community



Community Name Enter 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 FortiManager 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** Enter 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. You need to do this if the SNMP manager is on the Internet or behind a router.
- **Delete icon** Select to remove this SNMP manager.
- **Add** Select to add a new default entry to the Hosts list that you can edit as needed. You can have up to 8 SNMP manager entries for a single community.

Traps Enter the Remote port numbers (162 remote by default) that the FortiManager system uses to send SNMP v1 and SNMP v2c traps to the FortiManager in this community. Enable traps for each SNMP version that the FortiManager system uses.

SNMP Event Enable the events that will cause the FortiManager unit to send SNMP traps to the community. These events include:

- Interface IP changed
- Log disk space low
- HA Failover
- System Restart

Fortinet 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 Fortinet 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 Table 2 along with the two RFC MIBs. You can obtain these MIB files from Fortinet technical 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.

Table 2: Fortinet MIBs

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 “Fortinet traps” on page 55 and “Fortinet & FortiManager MIB fields” on page 56.
FORTINET-FORTIMANAGER-MIB.mib	The proprietary FortiManager MIB includes system information and trap information for FortiManager units. For more information, see “Fortinet & FortiManager MIB fields” on page 56.
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.

Fortinet 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 hostname (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.

Table 3: Generic Fortinet traps

Trap message	Description
ColdStart WarmStart LinkUp LinkDown	Standard traps as described in RFC 1215.

Table 4: Fortinet system traps

Trap message	Description
CPU usage high (fnTrapCpuThreshold)	CPU usage exceeds 80%. This threshold can be set in the CLI using `config system global`.
Memory low (fnTrapMemThreshold)	Memory usage exceeds 90%. This threshold can be set in the CLI using `config system global`.
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.

Table 5: FortiManager HA traps

Trap message	Description
HA switch (fmTrapHASwitch)	FortiManager HA 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.

Table 6: System MIB fields

MIB field	Description
fnSysSerial	Fortinet unit serial number.

Table 7: 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.

Table 8: Custom messages

MIB field	Description
fnMessages	The number of custom messages on the Fortinet unit.

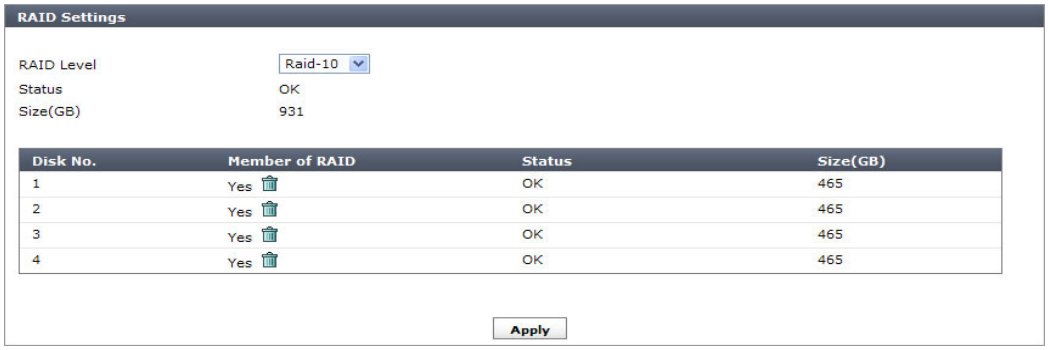
Table 9: FortiManager MIB fields and traps

MIB field	Description
fmModel	A table of all FortiManager models including: • fmg100 - FortiManager model 1000 • fmg400 - FortiManager model 4000 • fm400A - FortiManager model 4001 • fm2000XL - FortiManager model 20000 • fmg3000 - FortiManager model 30000 • fmg3000B - FortiManager model 30002
fmTrapHASwitch	The FortiManager HA cluster has been re-arranged. A new master has been selected and asserted.

RAID

RAID (Redundant Array of Independent Disks) helps to divide data storage over multiple disks. By dividing data this way, data reliability is increased. If your FortiManager unit has more than one hard disk (typically, the FortiManager-3000B or higher), you can enable RAID by going to *System Settings* > *General* > *RAID*, select a *RAID level* and select *Apply*.

Figure 19: Select the RAID options



Once selected, depending on the RAID level, it may take a while to generate the RAID array.

The FortiManager unit supports the following RAID levels 0,1, 5, and 10.

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 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 10

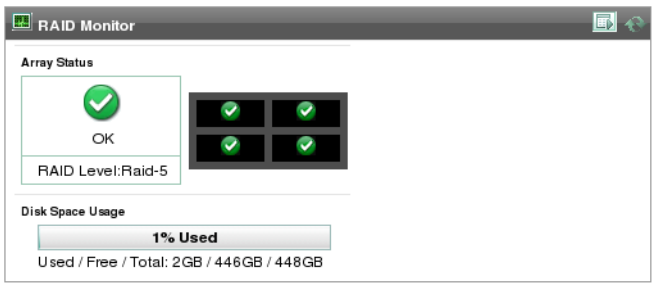
RAID 10 (or 1+0), includes nested RAID levels 1 and 0, or a stripe (RAID 0) of mirrors (RAID 1). The total disk space available is the total number of disks in the array (a minimum of 4) divided by 2. One drive from a RAID 1 array can fail without the loss of data; however, should the other drive in 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 Monitor widget

The RAID Monitor widget, on the dashboard (*System Settings* > *General* > *Dashboard)*, displays information about the status of RAID disks as well as what RAID level has been selected. The RAID Monitor also displays how much disk space is being used.

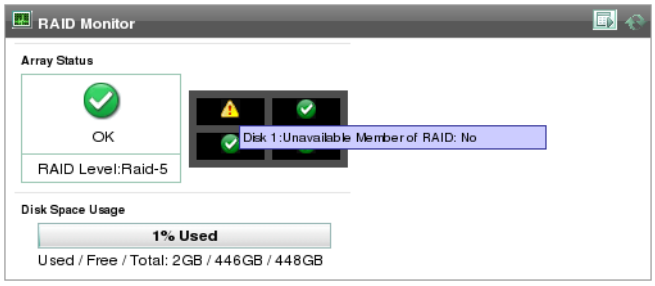
The RAID Monitor layout is similar to the look of the front panel. The Drive Status Indicator allows you to view each disk's name and the amount of space in GB each has. For example, Disk 2: Ready 465.76GB.

Figure 20: RAID Monitor displaying a RAID array without any failures



The Drive Status Indicator will also indicate when a disk has failed. This is displayed by both a warning symbol and text. The text appears when you hover your mouse over the warning symbol. When a disk has failed, caution triangle icon appears in the Drive Status Indicator.

Figure 21: RAID Monitor displaying a failed disk



Network settings

Network settings enable you to configure the basic network components to get the FortiManager unit on the network.

To configure the network settings, go to *System Settings* > *General* > *Network* to configure how your FortiManager unit connects to the network. You can configure:

- FortiManager unit interfaces
- routing tables
- DNS servers

Network interface

The FortiManager unit can manage Fortinet devices connected to any of its interfaces. The only exception being if the FortiManager unit is operating as part of an HA cluster, in which case, the interface used for HA operation is not available for other uses.

Figure 22: Network Interface list

	Name	IP/Netmask	Administrative Access	Service Access	Enable
☐	port1	172.20.120.175 / 255.255.255.0	HTTPS, HTTP, PING, SSH		✓
☐	port2	0.0.0.0 / 0.0.0.0			✓
☐	port3	0.0.0.0 / 0.0.0.0			✓
☐	port4	0.0.0.0 / 0.0.0.0			✓
☐	port5	0.0.0.0 / 0.0.0.0			✓
☐	port6	0.0.0.0 / 0.0.0.0			✓

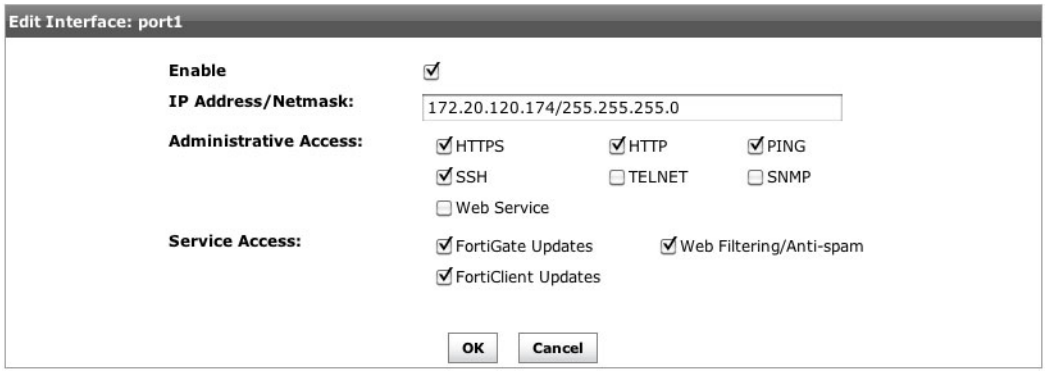
Name	The names of the physical interfaces on your FortiManager unit. The name, including number, of a physical interface depends on the model. Unlike FortiGate, you cannot set alias names for the interfaces. For more information, on configuring the interface, see "Configure network interfaces" on page 60. If HA operation is enabled, the HA interface has */HA* appended to its name.
IP / Netmask	The IP address and netmask associated with this interface.
Administrative Access	The list of allowed administrative service protocols on this interface. These include HTTP, HTTPS, PING, SSH, and Telnet.

Service Access	The list of Fortinet services that are allowed access on this interface. These include FortiGate updates, FortiClient updates, Web filtering, and Antispam. By default all service access is enabled on port1, and disabled on port2.
Enable	Displays if the interface is enabled or disabled. If the port is enabled, a green circle with a check mark appears in the column. If the interface is not enabled, a gray circle with an "X" appears in the column.

Configure network interfaces

Go to *System Settings* > *Network* > *Interface* and select the interface name link to change the interface options.

Figure 23: Configure network interfaces

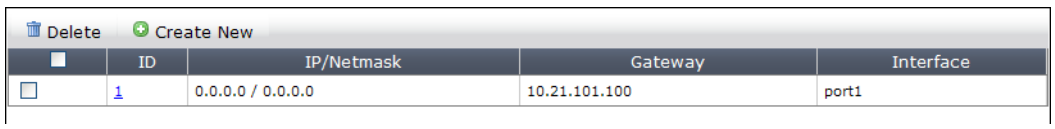


Enable	Select to enable this interface. A green circle with a check mark appears in the interface list to indicate the interface is accepting network traffic. When not selected, a gray circle with an "X" appears in the interface list to indicate the interface is down and not accepting network traffic.
IP Address/Netmask	Enter the IP address and netmask 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 web-manager access or SSH for CLI access.
Service access	Select the services that will communicate with this interface.

Routing table

Go to *System Settings* > *Network* > *Static Routing* to view, edit, or add to the static routing table. You may need to add entries to the routing table so that the FortiManager unit can reach FortiGate units on remote networks.

Figure 24: Routing Table



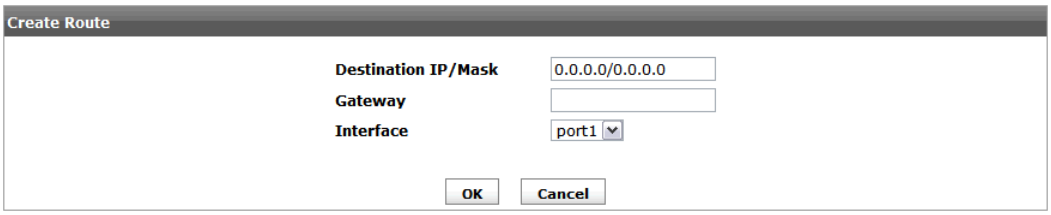
Create New	Select *Create New* to add a new route. See "Adding a route" on page 61. Select the route number to edit the settings.
Delete	Select the check box next to the route number and select Delete to remove the route from the table.
ID	The route number.
IP/Netmask	The destination IP address and netmask for this route.

Gateway	The IP address of the next hop router to which this route directs traffic.
Interface	The network interface that connects to the gateway.

Adding a route

Go to *System Settings* > *Network* > *Static Routing* and select *Create New* to add a route or select the route number to edit an existing route.

Figure 25: Create New route



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

Configuring DNS

Go to *System Settings* > *Network* > *DNS* to configure the DNS servers that the FortiManager unit uses. The DNS servers must be on the networks to which the FortiManager unit connects, and should be two different addresses.

Primary DNS Server	Enter the primary DNS server IP address.
Secondary DNS Server	Enter the secondary DNS server IP address.

Configuring administration settings

The administration settings provide a location to configure global settings for administrator access to the FortiManager unit, including the level of access, which administrative domains users have access to, and setting up profiles which define an administrators access. All administrator settings can only be configured when you are logged in as the `admin` administrator. The `admin` administrator is the only user with complete access to the entire FortiManager system options.

Go to *System Settings* > *General* > *Administration* to:

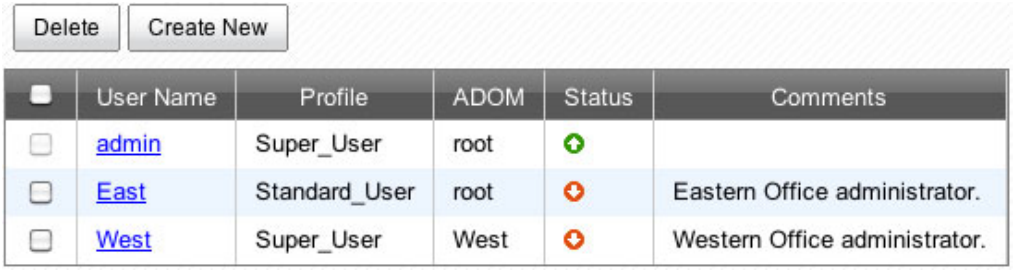
- configure ADOMs
- create and edit administrators
- create and edit administrator profiles
- monitor administrator sessions
- change device lock settings
-

Administrator list

Go to *System Settings* > *Administration* > *Administrator* to view the list of administrators and configure administrator settings.

The default `admin` administrator account has full privileges and will see the complete administrators list. If you do not have certain viewing privileges, you will not see the administrator list.

Figure 26: Administrator list

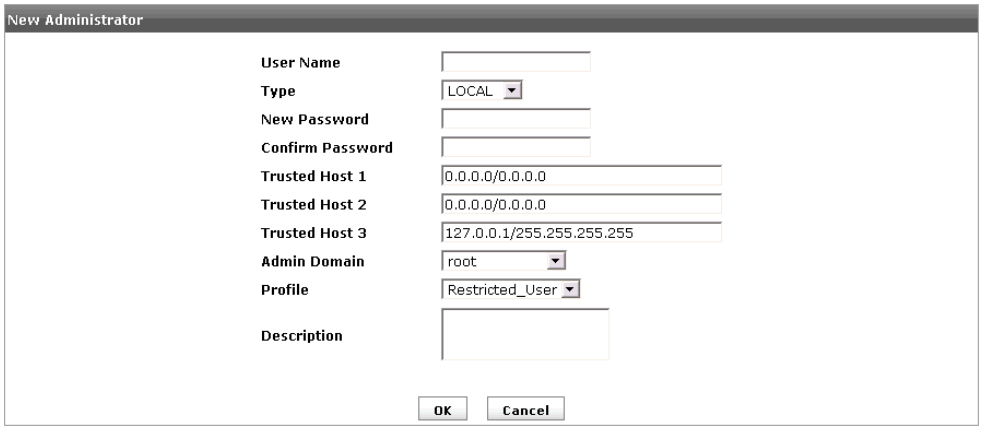


Create New	Select to create a new administrator. For more information, see "Adding an administrator" on page 62.
Delete	Select the checkbox next to the administrator you want to remove from the list and select Delete.
User Name	The name this administrator uses to log in. Select the administrator name to edit the administrator settings.
Profile	The administrator profile for this user that determines the privileges of this administrator. For information on administrator profiles, see "Administrator profile" on page 63.
ADOM	The ADOM to which the administrator has been assigned.
Status	Indicates whether the administrator is currently logged into the FortiManager unit not. A green circle with an up arrow indicates the administrator is logged in, a red circle with a down arrow indicates the administrator is not logged in.
Comments	Descriptive text about the administrator account.

Adding an administrator

Go to *System Settings* > *Administration* > *Administrator* and select *Create New* to add a new administrator account.

Figure 27: Administrator account settings



User Name	Enter the name that this administrator uses to log in. This field is available if you are creating a new administrator account.
Type	Select the type of authentication the administrator will use when logging into the FortiManager unit. If you select *LOCAL*, you will need to add a password. Otherwise, depending on the type of authentication server selected, you will select the authentication server from a drop-down list.
Change Password	Select to change passwords. This is available if *Type* is *LOCAL*, and you are editing an existing administrator account.
Old Password	Enter your old password. This is available only if *Type* is *LOCAL*, and you are editing the current administrator account.
New Password	Enter the password. This is available if *Type* is *LOCAL*.
Confirm Password	Enter the password again to confirm it. This is available if *Type* is *LOCAL*.
Trusted Host1 **Trusted Host2** **Trusted Host3**	Optionally, enter the trusted host IP address and netmask from which the administrator can log in to the FortiManager unit. You can specify up to three trusted hosts. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see "Using trusted hosts" on page 63.
Admin Domain	Choose the Administrative Domain this admin will belong to. This field is available only if administrative domains are enabled. For more information on enabling administrative domains, see "Enabling administrative domains" on page 36.
Profile	Select a profile from the list. The profile selected determines the administrator's access to FortiManager unit features. To create a new profile see "Administrator profile" on page 63.
Description	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.

Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. 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.

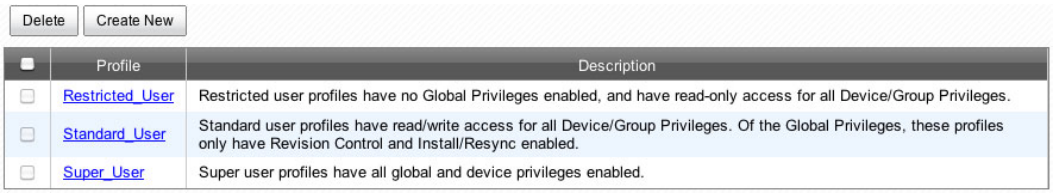
When you set trusted hosts for all administrators, the FortiManager unit does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply both to the web-based manager and to the CLI when accessed through SSH. CLI access through the console connector is not affected.

Administrator profile

Go to *System Settings* > *Administration* > *Profile* to create or edit administrator profiles.

Figure 28: Administrator profile list



Create New	Create a new administrator profile. See "Administrator profile" on page 63.
Delete	Select the checkbox next to the profile to delete and select *Delete*. Predefined profiles cannot be deleted. You can only delete custom profiles when they are not applied to any administrators.
Profile	The administrator profile name. Select the profile name link to edit the existing settings.
Description	Moving the mouse over the *Description* Icon brings up the tool tip for the description field after a short delay. If there is no description for that profile, no icon appears.

There are three pre-defined profiles with the following privileges:

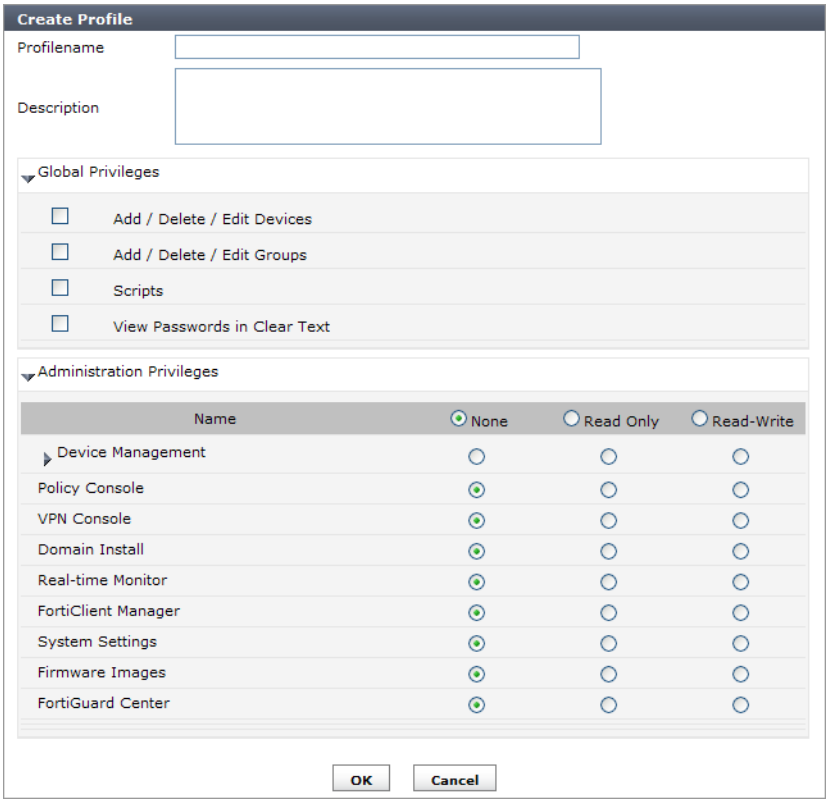
Super_User	Super user profiles have all system and device privileges enabled.
Standard_User	Standard user profiles have no System Privileges enabled, but have read/write access for all Device Privileges.
Restricted_User	Restricted user profiles have no System Privileges enabled, and have read-only access for all Device Privileges.

You cannot delete these profiles, but you can modify them.

To create a new administrator profile go to *System Settings* > *Administration* > *Profile* and select *Create New*.

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

Figure 29: Administrator profiles settings



Profile Name	Enter a name for this profile.
Description	Enter a description for this profile. While not a requirement, a description can help to know what the profiles is for or the levels it is set to.
Global Privileges	Expand this section and select the privileges for this administrator, as required.
Administration Privileges	Expand this section. Select *None*, *Read Only* or *Read-Write* access for categories as required. The administration privileges available are: • Device Management • Policy Console • VPN Manager • Domain Install • Real-time Monitor • FortiClient Manager • System Settings • Firmware Images • FortiGuard Center Select the expand arrow for *Device Management* for more fields. These detailed fields inherit privileges selected at the top level.

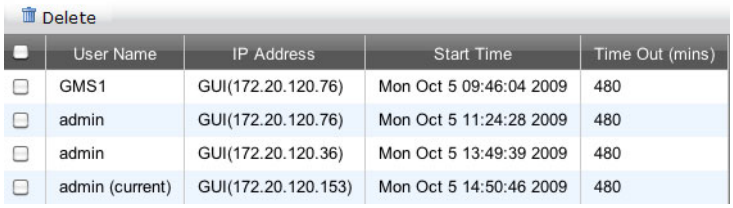
Monitoring administrator sessions

Through the administrator options you can view the list of administrators logged into the FortiManager unit. The *Logged-In Session* view enables you to determine who is on the system should you need to upgrade or reboot the FortiManager and let the administrator know that, or when, the system is going down or being rebooted.

From this window you can also disconnect users if necessary.

To view the administrators on the FortiManager unit, go to *System Settings* > *Administration* > *Logged-In Session*.

Figure 30: Administrator session list



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.
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).
Delete	Select the check box next to the user and select Delete to drop their connection to the FortiManager unit.

To disconnect an administrator

1 Go to *System Settings* > *Administration* > *Logged-In Session*.

2 Select the checkbox next to the administrator(s) to disconnect, and select *Delete*.

3 Select *OK* to confirm deletion of the session.

The disconnected administrator will see the FortiManager login 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.

Note: Disconnecting an administrator will reset any configuration locks set by that administration session.

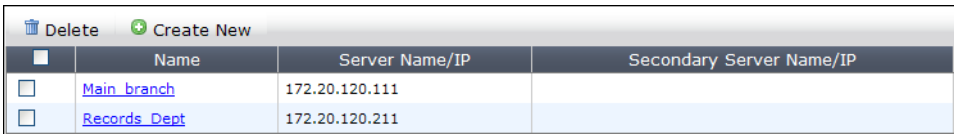
RADIUS server

Remote Authentication Dial-in User (RADIUS) is a user authentication and network-usage accounting system. When users connect to a server they enter 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 RADIUS 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.

Go to *System Settings* > *Administration* > *Radius Server* to create a new RADIUS server entry or edit an existing entry.

Figure 31: RADIUS server list



Create New	Add a new RADIUS server entry.
Delete	Select the check box next to the server entry and select *Delete*. You cannot delete a RADIUS server entry if there are administrator accounts using it.
Name	The RADIUS server name. Select the server name to edit the settings.
Server Name/IP	The IP address or DNS resolvable domain name of the RADIUS server.
Secondary Server Name/IP	Optional IP address or DNS resolvable domain name of the secondary RADIUS server.

To add a RADIUS server, go to *System Settings* > *Administration* > *Radius Server* and select *Create New* to create a new RADIUS server configuration.

Figure 32: RADIUS configuration

Name	Enter a name to identify the RADIUS server.
Server Name/IP	Enter the IP address or fully qualified domain name of the RADIUS server.
Server Secret	Enter the RADIUS server secret.
Secondary Server Name/IP	Enter the IP address or fully qualified domain name of the secondary RADIUS server.
Secondary Server Secret	Enter the secondary RADIUS server secret.
Port	Enter the port for RADIUS traffic. The default port is 1812. You can change it if necessary. Some RADIUS servers use port 1645.
Auth-Type	Enter the authentication type the RADIUS server requires. The default setting of *ANY* has the FortiManager unit try all the authentication types.

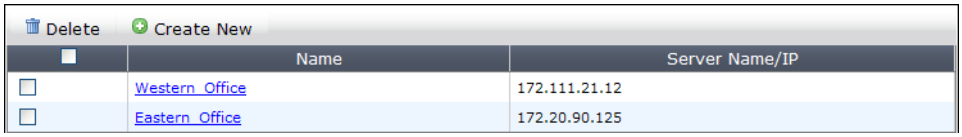
LDAP server

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.

Go to *System Settings* > *Administration* > *LDAP Server* to create a new LDAP server entry or edit an existing server entry.

Figure 33: LDAP server list



Delete	Select the check box next to the server name and select *Delete*. You cannot delete a LDAP server entry if there are administrator accounts using it.
Create New	Add a new LDAP server entry.
Name	The LDAP server name. Select the server name to edit the settings.
Server Name/IP	The IP address or DNS resolvable domain name of the LDAP server.

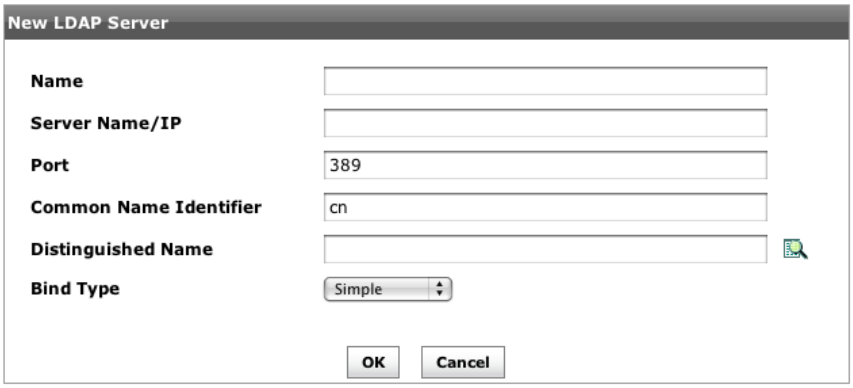
To add a LDAP server

1 Go to *System Settings* > *Administration* > *LDAP Server.*

2 Select *Create New* to create a new LDAP server configuration.

3 Enter the following information.

Figure 34: LDAP configuration



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

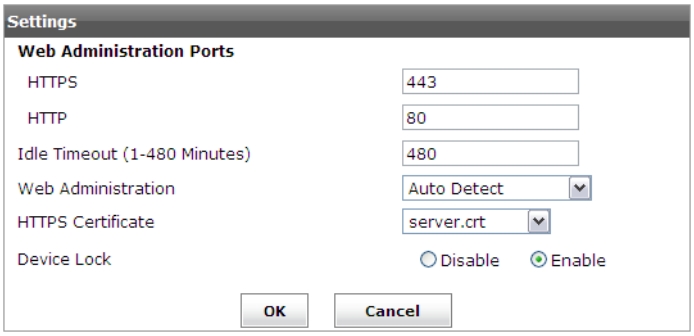
Administrative settings

The administrative settings are where you set the basic global options that apply to all administrators logging onto the FortiManager unit. These options include

- Ports for HTTPS and HTTP administrative access
- Idle Timeout settings
- Language of the web-based manager
- Device lock

To configure the administrative settings, go to *System Settings* > *Administration* > *Admin Settings*.

Figure 35: Administrative settings



HTTPS	Enter the TCP port to be used for administrative HTTPS access.
HTTP	Enter the TCP port to be used for administrative HTTP access.
Idle Timeout	Enter 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.
Web Administration	Select a language for the web-based manager to use. When set to *Auto Detect*, the FortiManager unit detects the language settings of your web browser.
HTTPS Certificate	Select the certificate that is used for secure connections.
Device Lock	Select enable to enable device configuration locking. This enables an administrator to lock a FortiGate unit so that no other administrator can make changes while the current administrator is editing the FortiGate unit options until that lock is released. This will ensure there is no conflicting settings or wiping out the new configurations. For more information see “Device configuration locks” on page 69.

Device configuration locks

Device configuration locks enables an administrator to prevent other administrators from modifying individual FortiGate unit settings.

This lock prevents problems that occur when two people make different changes to the same unit at the same time. Once the administrator who locked the unit has completed the changes, their device configuration lock can be safely removed and everyone will have access to the updated unit as normal. You need to enable device locks to lock a device or device group.

To enable device locks

1 Log in as the `admin` administrator (the super user account).

2 Go to *System Settings* > *Administration* > *Admin Settings*.

3 Select *Enable* for *Device Lock*.

4 Select *OK*.

When the device configuration lock feature is enabled there is a change in the appearance of the web-based manager and also in device behavior.

When device configuration locks are enabled, a padlock icon will appear beside the FortiGate units in the summary window.

If the device is currently locked by an administrator, it will appear as a closed padlock. Otherwise the icon appears as an open padlock.

The super administrator can unlock device locks set by other administrators or simply end their session. By default if the session has no activity for more than 60 minutes, the lock will automatically be removed.

Device group locks

The device group lock enables you to lock an entire group of devices at once instead of locking them one at a time. Once locked or unlocked, you can still lock or unlock individual devices in the group.

To lock a device group, in *Device Manager* select the group that you want to lock and select *Lock All*.

Device behavior

When device configuration locks are enabled, the behavior of the FortiManager unit and how you work with devices changes.

If an administrator is working with a device and its configuration, that administrator can lock that device while making their changes to avoid conflicting updates or changes. When the changes are complete, that administrator unlocks the device and everyone can access the device as normal.

While the device is locked, other administrators cannot access its configuration to change it. This ensures only one person is making changes at any given time.

The lock is by administrator account and session. If the same administrator account is logged onto the FortiManager system with two different sessions and one has locked a device, the other session will not be able to access that device.

To change a device configuration with device locks enabled

1 Go to *Device Manager* > <*device_type*>.

For example, to see FortiGate devices, go to *Device Manager* > *FortiGate.*

2 In the device summary table, lock a device by selecting the open padlock icon.

The icon will change to a closed padlock when the device has been locked.

3 Make your changes and commit them.

4 Unlock the chosen device by selecting the closed padlock icon.

The device is available to all administrators again once the padlock icon appears open. It is good practice to confirm this.

Local log settings

The FortiManager unit includes a system to view the events and activities occurring on the device through its log files. The FortiManager logging provides a number of options to record system events. Events that FortiManager can log include:

- System manager event
- FG-FM protocol event
- Device configuration event
- Global database event
- Script manager event
- Web portal event
- Firewall objects event
- Policy console event
- VPN console event
- Endpoint manager event
- Revision history event
- Deployment manager event
- Real-time monitor event
- Log and report manager event
- HA event
- Firmware manager event
- FortiGuard service event
- FortiClient manager event
- FortiMail manager event
- Debug I/O log event
- Configuration change event

The FortiManager unit can save log messages to the internal hard disk, memory or send them to a FortiAnalyzer unit. The events selected are the events that will generate messages in the local log files.

To select which events to log

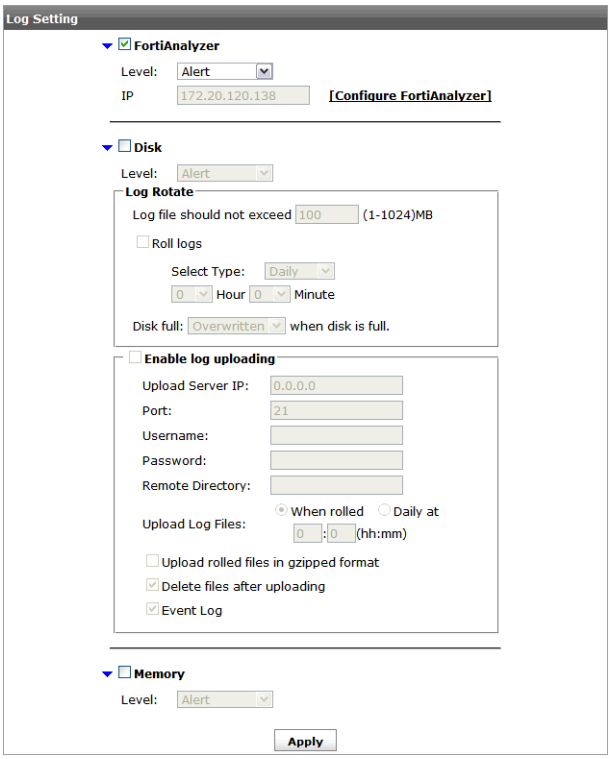
1. Go to *System Settings* > *Local Log* > *Event Log*.
2. Select *Enable*.
3. Choose which events to log by selecting from the events listed.
4. Select *Apply*.

Log settings

Through the log settings you set where the FortiManager unit stores the local log information from the options selected in the Event Log. With FortiManager, you can store logs to memory, the local hard disk, or send them to a FortiAnalyzer unit. You can send the logs to one, two or all of these locations, depending on your requirements.

To configure where the FortiManager sends the local event logs, go to *System Settings* > *Local Log* > *Log Setting*.

Figure 36: Configure Log settings



FortiAnalyzer	Select to send event logs to a FortiAnalyzer unit. Select the expand arrow to display options for FortiAnalyzer.
Level	Select the severity level of event reporting from *Emergency* (only emergency events are logged) to *Information* (all event levels are logged). This drop-down list is only available when the *FortiAnalyzer* checkbox is selected.
IP	The IP address of the FortiAnalyzer unit.
[Configure FortiAnalyzer]	Select to configure the FortiAnalyzer settings. For more information on configuring the connection to a FortiAnalyzer unit, see "Send logs to a FortiAnalyzer unit" on page 73.
Disk	Select to send event logs to the internal hard disk. Select the expand arrow to display the options for logging to the hard disk.
Level	Select the severity level of event reporting from *Emergency* (only emergency events are logged) to *Information* (all event levels are logged). This drop-down list is only available when the *Disk* checkbox is selected.
Log file should not exceed	Enter the maximum file size in megabytes for the event log file.
Rotate logs	Select to enable log file rolling. When the FortiManager unit rolls a log, the file is saved as a new file name, and a new file is started. Old log files can be uploaded to a remote server for storage as a backup.
Select Type	Select schedule when the FortiManager unit rolls the log files.
Select One Day	This field appears if *Select Type* is set to *Weekly.* Select the day of the week when the FortiManager unit rolls the logs.

Hour/Minute	This field is available when *Enable logfile rolling* is enabled. Enter the time of day to roll the logs. Hours and minutes are in two digit 24-hour format.
Disk Full	Select what action the FortiManager should take if the internal log disk becomes full. Selecting *Overwritten* will cause the FortiManager unit to continue to log to the hard disk, and erase previous event logs stored to disk. Select *Do not log* to prevent the overwriting of logs. Note that when this option is selected, the FortiManager will no longer log to the hard disk.
Enable log uploading	Select to enable event logs to be uploaded to a remote server. With this option, you can define the frequency of the uploading of log files, which can prevent the local hard disk becoming full, and potentially stop logging or overwriting of log files.
Upload server IP	Enter the IP address of the server where the logs are uploaded to.
Port	Enter the upload server's port number where the logs are uploaded to.
Username	Enter the username to use to connect to the upload server.
Password	Enter the password to use to connect to the upload server.
Remote directory	Enter the directory on the upload server where the logs are stored. The directory can be a maximum of 31 characters long. The FortiManager unit does not allow spaces in directories.
Upload log files	Select the frequency when the FortiManager unit uploads the log files. If *Daily* is selected, enter the hour and minute to upload log files in two digit 24-hour format.
Upload rolled files in gzipped format	Select to reduce the size of the uploaded log files by compressing them with the gzip utility.
Delete files after uploading	Select to delete log files after they have been uploaded. With this selection enabled, once the logs are uploaded, the files are deleted, avoiding the potential of a full hard disk.
Event Log	Currently enabled and unavailable for disabling. The Event log is currently the only log type created by the FortiManager unit.
Memory	Select to enable Event logs to be stored in memory. Select the expand arrow to display the options for logging to the FortiManager memory. The FortiManager unit has limited space for logging to memory, and has not method of backing up or saving
Level	Select the severity level of event reporting from *Emergency* (only emergency events are logged) to *Information* (all event levels are logged). This drop-down list is only available when the *Memory* checkbox is selected.

Send logs to a FortiAnalyzer unit

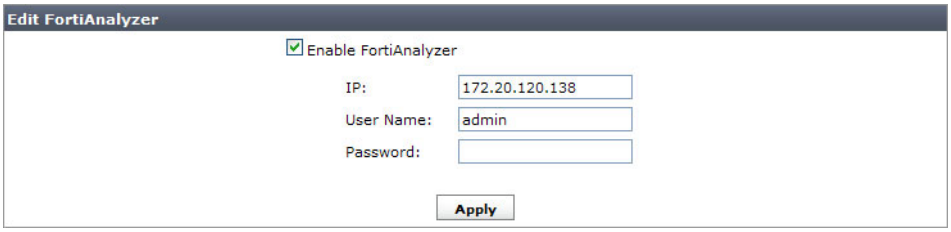
FortiAnalyzer units are network devices that provide integrated log collection, analysis tools and data storage. Detailed log reports provide historical as well as current analysis of network activity to help identify security issues and reduce network misuse and abuse.

The FortiAnalyzer unit enables you to remotely store FortiManager Event logs and to run reports on the activities of the FortiManager and other devices.

To configure the FortiManager unit to send logs to a FortiAnalyzer unit

1. Go to *System Settings* > *Local Log* > *Log Setting*.
2. Select *[Configure FortiAnalyzer]*.
3. Enter the following information:

Figure 37: FortiAnalyzer settings



Enable FortiAnalyzer	Select to enable the connection to a FortiAnalyzer unit.
IP	Enter the IP address of the FortiAnalyzer unit.
User Name/Password	Enter a user name and password the FortiManager unit can use to log in to the FortiAnalyzer unit.

To establish a connection between the FortiManager and FortiAnalyzer

1. On the FortiAnalyzer unit, go to *System* > *Network* > *Interface*.
2. Select *Edit* for the port connected to the network.
3. Select *WEB SERVICES*.
4. Select *OK*.
5. On the FortiManager unit go to *System Settings* > *Local Log* > *Log Setting.*
6. Select *Configure FortiAnalyzer*.
7. Select *Enable FortiAnalyzer*.
8. Enter the IP address, login username and password of the FortiAnalyzer unit.
9. Select *Apply*.

The next event to be logged will register the FortiManager unit on the FortiAnalyzer unit's unregistered device list. At that point, you can optionally enable, block, or delete the FortiManager unit. Once it has been enabled, subsequent events are logged by the FortiAnalyzer unit.

Send logs to the local hard disk

The FortiManager can write Event logs to its local hard disk. When sending logs to the hard disk, the logs can become quite large. If they become too large, they can become slow for data retrieval, and should the file become corrupted, you can lose all your log information.

To configure the FortiManager unit to send logs to a FortiAnalyzer unit, go to *System Settings* > *Local Log* > *Log Setting* and select *Disk* and select the log level.

When configuring the FortiManager unit to send logs to its hard disk, you can define the maximum size of the log file. When that size is reached, the FortiManager will rename the log file, and start a new log file. For example, the log file name on the hard disk that is always active is called elog. Once the file size has been reached, it rolls to the filename elog.1, elog.2 and so on. When viewing the log files (see "Log access" on page 75), the table display includes the last access time, which indicates when the last log was written to it.

At some point, the logs may fill the hard disk. When this happens, you can either instruct the FortiManager unit to overwrite the older logs, or stop logging until you can clear the hard disk.

To configure log rolling

1. Go to *System Settings* > *Local Log* > *Log Setting*.
2. Select *Disk*.
3. Set the maximum size of the log file.
4. Select *Roll Logs* and select the frequency when the FortiManager will roll the logs to a new file.
5. Select the action the FortiManager unit takes when the hard disk is full.
6. Select *OK*.

For long term storage, you can also upload rolled logs to an off-site server or FTP site.

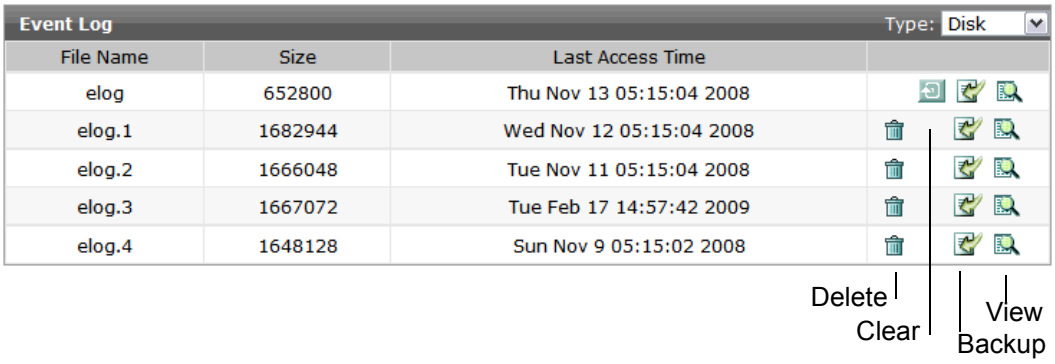
To upload logs to an off-site server, select *Enable Log Uploading* and complete the following:

Upload server IP	Enter the IP address of the server where the logs are uploaded to.
Port	Enter the upload server's port number where the logs are uploaded to.
Username	Enter the username to use to connect to the upload server.
Password	Enter the password to use to connect to the upload server.
Remote directory	Enter the directory on the upload server where the logs are stored. The directory can be a maximum of 31 characters long. The FortiManager unit does not allow spaces in directories.
Upload log files	Select the frequency when the FortiManager unit uploads the log files. If *Daily* is selected, enter the hour and minute to upload log files in two digit 24-hour format.
Upload rolled files in gzipped format	Select to reduce the size of the uploaded log files by compressing them with the gzip utility.
Delete files after uploading	Select to delete log files after they have been uploaded. With this selection enabled, once the logs are uploaded, the files are deleted, avoiding the potential of a full hard disk.

Log access

To view and manage logs, go to *System Settings* > *Local Log* > *Log Access*.

Figure 38: Event log



Type	Select *Disk* or *Memory* for the location of the event log.
File Name	The name of the event log file.
Size	The size of the event log file, in bytes.

Last Access Time	The date and time the event log was last accessed, or more specifically last saved.
Clear icon	Clear the current event log. This will remove all the entries in the current event log.
Backup icon	Select to backup the event log to the management PC hard disk in comma separated format or in its binary format.
View icon	Select to view the event log. You will view either the disk or memory event log as selected by *Type*.

To back up local event logs

1 Select the *Backup* icon.

2 Select one or more of:

Download file in the normal format	The event log will be in its raw format
Download the file in CSV	The event log will have its data separated by commas

3 Select *OK* to save the file.

Viewing local event logs

The logs created by FortiManager are viewable within the web-based manager. You can use the FortiManager Log Message Reference, available on the Fortinet Technical Documentation web site to interpret the messages. You can view log messages in the FortiManager web-based manager that are stored in memory or on the internal hard disk. To view log messages stored on a FortiAnalyzer unit, you need to view them from the FortiAnalyzer web-based manager.

To view the log messages

1 Go to *System Settings* > *Local Log* > *Log Access*.

2 Select the storage location by selecting it from the *Type* drop-down list in the upper right corner.

3 Select the *Browse* icon for the log file you want to view.

Advanced Metadata

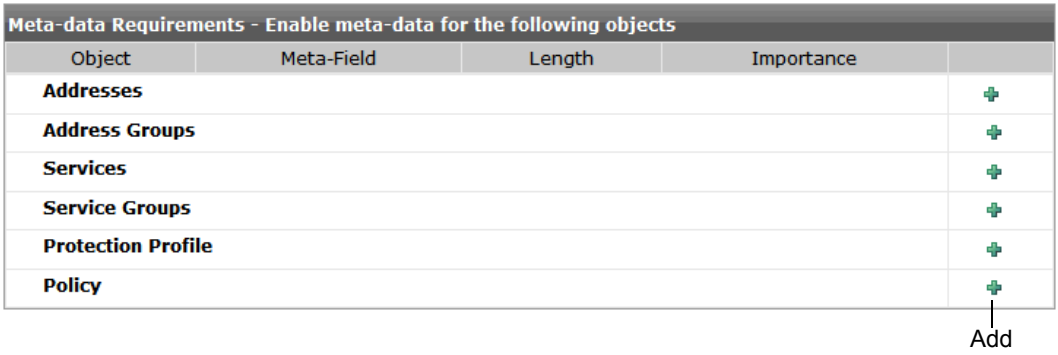
The FortiManager unit enables you and other administrators to add extra information when configuring, adding or maintaining FortiGate units or adding new administrators. You can make the fields mandatory or optional, and set the side of the field.

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 Administrators. This object applies to administrators on the FortiManager unit. All other objects are related to FortiGate units.

Go to *System Settings* > *Advanced* > *Meta Fields* > *System Objects Meta* to add metadata fields for system-wide objects, or select the *Config Objects Meta* tab to configure other objects. Administrators configure meta-data fields for administrator accounts, and the others configure fields for FortiGate objects.

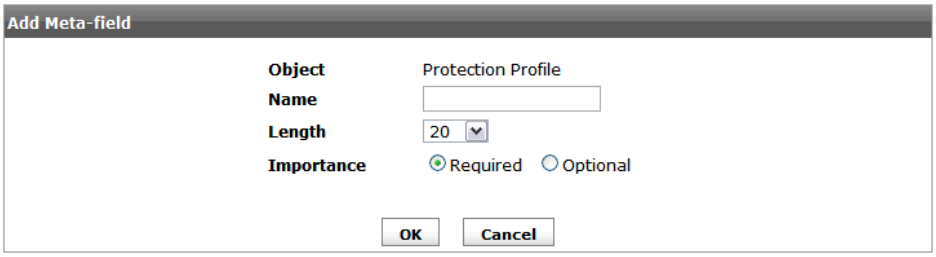
Figure 39: Config objects meta-data



Object	A FortiGate module object.
Meta-Field	The name of this meta-data field.
Length	The maximum length of this meta-data field.
Importance	Indicates whether this field is required or optional.
Add icon	Create a new meta-data field for this object.
Delete icon	Select to delete this meta-data field.
Edit icon	Select to edit this meta-data field.

To add a new metadata field, go to *System Settings* > *Advanced* > *Meta Fields* and select the *Add* icon for a FortiGate object to create a new meta-data field.

Figure 40: Add meta-field

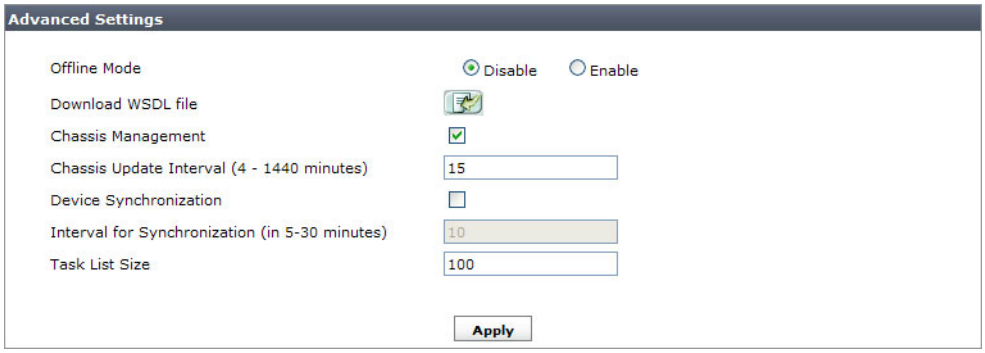


Object	The FortiManager or FortiGate object to which this metadata field applies.
Name	Enter the label to use for the field.
Length	Select the maximum number of characters allowed for the field.
Importance	Select *Required* to make the field compulsory, otherwise select *Optional*.

Advanced settings

To view the advanced settings options, go to *System Settings* > *Advanced* > *Advanced Settings*.

Figure 41: Advanced settings



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.
Download WSDL file	Select to download the FortiManager unit's Web Services Description Language (WSDL) file. 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 admin user would from the web-based manager or CLI.
Chassis Management	Select to enable Chassis management in Device Manager. This option is only available in FortiManager-3000 and higher. Chassis Management enables you to monitor and maintain a FortiGate-5050 or FortiGate-5140 chassis, through the shelf manager on the chassis. Through the configuration, you can monitor the shelf manager, blade and chassis status and alarms. For more information, see "Working with Shelf Manager" on page 112. For information on connecting to and configuring the shelf manager, see the FortiGate-5050 or FortiGate-5140 Chassis Guide.
Chassis Update Interval	Set the time interval for the FortiManager to check for the shelf manager status.
Device Synchronization	Select to enable FortiManager to synchronize the settings you make with the managed devices.
Interval for synchronization	Select the time interval in minutes between synchronizations with devices.
Task List Size	Set a limit on the size of the Task List.

Firmware images

Your FortiManager can store firmware images for the FortiGate, FortiAnalyzer, and FortiManager devices it is connected to. You can use your FortiManager unit to roll out updated firmware images to those units. If you purchase a FortiGuard subscription, you can even automate the process of downloading updated firmware images and upgrading the units connected to the FortiManager unit.

You can view the firmware images stored on the FortiManager unit and download new firmware images from the FDN by going to *System Settings* > *Firmware Images*. You must have root administrative privileges to view *System Settings* > *Firmware Images*.

The *Firmware Images* option does not appear in GMS mode. For more information, see "Changing Firmware" on page 271.

FortiGuard Center

The default behavior of each FortiGate, FortiAnalyzer, and FortiManager unit is to directly contact the nearest FDN server for IPS and AntiVirus updates. To save network bandwidth and perhaps simplify your network configuration, you can configure your FortiManager unit to act as an FDN server. Your FortiManager unit retrieves the updates from the nearest FDN server for updates, and all your other units will contact your FortiManager unit for the updates.

The *FortiGuard Center* option does not appear in GMS mode.

For more information and configuration instructions, see "FortiGuard Center" on page 250.

Managing Devices

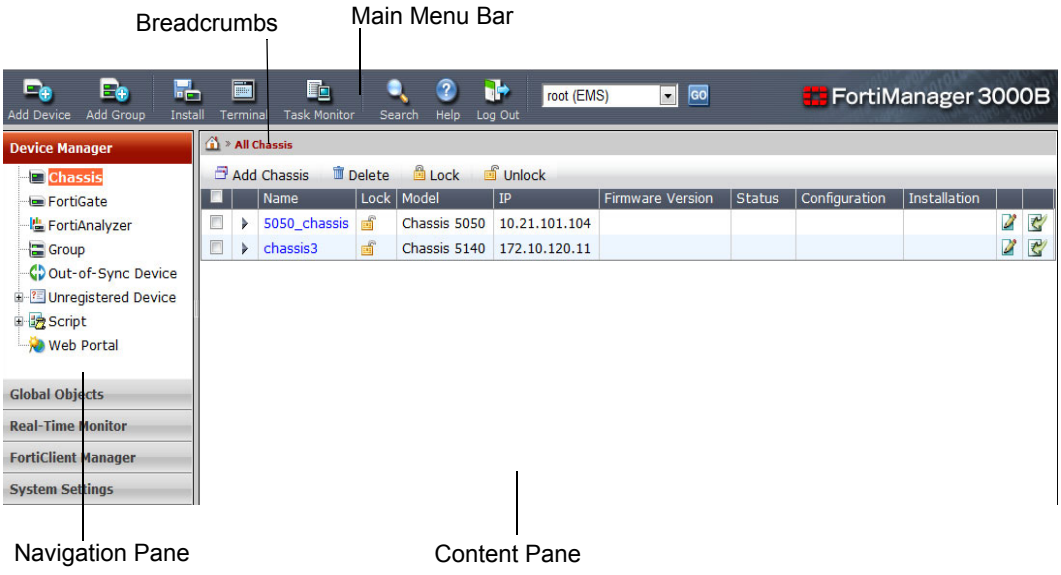
Use the *Device Manager* window to add FortiGate, FortiSwitch, FortiOS Carrier, FortiMail, and FortiAnalyzer units to the FortiManager system. Once you have added the devices and organized them into groups, you can configure single devices or groups of devices.

This section describes:

Device Manager window

The *Device Manager* window includes breadcrumbs, Main Menu Bar, Navigation Pane, and Content Pane. This is the default window for the FortiManager system.

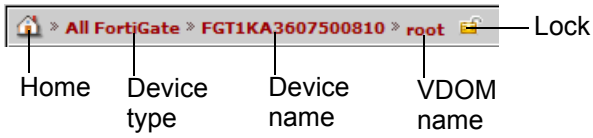
Figure 42: Sample Device Manager window in EMS mode



Breadcrumbs

Breadcrumbs, also known as navigation history, displays the sequence of items you selected to reach your current display - the top level, the device type, the device name, and VDOM name, if applicable. This allows you to easily jump back to any point along that path for easier navigation. This area also displays a home icon to return to the top level and a lock icon to display if a device is locked or unlocked.

Figure 43: Navigation history



For example if you are looking at a FortiGate unit called `myFortiGate` with a VDOM called `vdom1`, and you are looking at firewall policies the breadcrumbs will display all that information. If you want to change to a different VDOM on that same FortiGate unit, you could select the level above the VDOM and choose another VDOM from the list.

Main menu Bar

Use the Main Menu Bar buttons to manage devices or perform system tasks. The Main Menu bar displayed for nearly all windows in the Navigation Pane is the Device Manager Main Menu Bar.

When you detach the Security Console window, it has a different Main Menu Bar. See “Detach Security Console” on page 198.

When you are in FortiClient Manager, it has a different Main Menu Bar again. See “Main Menu Bar” on page 304.

Figure 44: Main Menu Bar

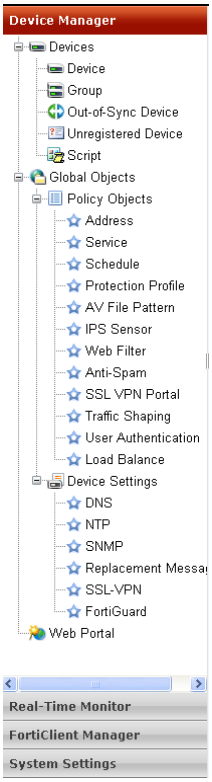
Add Device	Select to add a FortiGate, FortiAnalyzer, or FortiMail unit to the current administration domain. See “Adding a device” on page 84.
Add Group	Select to add a group of FortiGate devices to the current administration domain. See “Adding FortiGate groups” on page 95
Install	Select to install changes from the FortiManager database to the physical devices. Optionally install to FortiGate or FortiCarrier units. See “Installing Device Configurations” on page 277. Optionally select to perform Security Domain activities such as copy, install, or review policies. See “Security Console window” on page 197.
Terminal	Select to open a terminal connection to a device. For more information on connecting to managed devices, see “Using the CLI console for managed devices” on page 104.
Task Monitor	Select to view current or past tasks the FortiManager system is performing or has performed grouped by status. See “Using the task monitor” on page 104.
Search	Select to search for information in global objects. See “Searching for global objects” on page 106.
Help	Select to view the online help for the current display.
Log Out	Select to log out of the FortiManager web-based manager.

ADOM drop-down menu	Select an administrative domain activate. Optionally select Manage ADOMs to create, edit, or delete administrative domains. See “Administrative Domains” on page 33.
GO	Select to activate your selection in the ADOM drop-down menu.

Navigation Pane

In the *Device Manager* section of the Navigation Pane, you can select and view the configuration options associated with devices, global objects, and (EMS mode only) web portals.

Figure 45: Navigation Pane (EMS mode)



The Navigation Pane has the following items:

Device Manager	Select to display device configuration options.
Chassis	Select to display the list of FortiGate-5000 units.
FortiGate	Select to display the list of all non-FortiGate-5000 models of FortiGate and FortiWifi units.
FortiMail	Select to display a list of all FortiMail units.
FortiAnalyzer	Select to display a list of all FortiAnalyzer units.
Group	Device groups registered with the FortiManager system.
Out-of-Sync Device	Devices with configurations that are not synchronized with the FortiManager system.
Unregistered Device (EMS only)	Devices that have not been added to the FortiManager system as managed units, but have been configured through their own web-based manager or CLI to be managed by this FortiManager system. EMS mode only.

Script	Scripts for a device or a group. For more information, see “Working with Scripts” on page 223.
Web Portal	Select to configure an on-the-device customizable web portal that customers can use to rebrand and redesign the configuration GUI. For more information, see “Administrative Web Portal” on page 209.
Global Objects	Select to display:
Policy Objects	Global firewall policy configurations (EMS mode only). For more information, see “Configuring global policy objects” on page 128.
Device Settings	Basic device configurations that can be shared globally. For more information, see “Configuring global device settings” on page 186.

Content Pane

When you select an item in the Navigation Pane, the information is displayed in the Content Pane. This includes lists of devices or objects, screens to create or edit devices or obejcts, and other configuration related tasks. The Content Pane features a menu bar at the top, in addition to the Main Menu Bar. The Content Pane menu bar includes buttons to perform basic tasks such as create, edit, delete, and search. The options on the menu can change depending on what task you are performing, and what infomration is being displayed.

Adding a device

To manage a device, you must add it to the FortiManager system. You can add an existing operational device or an unregistered device.

You can also add devices singly or add multiple devices all at once. Although they function in the same way, you cannot select the device discovery method and enter device description when adding multiple devices. *Auto Discover* is the defaulted method for adding multiple devices.

Before you can connect a device to the FortiManager system, you must configure the device. For detailed information, see the *FortiManager Installation Guide*.

For an existing device, use the *Add Device* function and provide its IP address. The FortiManager system determines the model and firmware version. Adding an existing device will not result in an immediate connection to the device. Device connection happens only when you successfully resync the device.

Unregistered devices have already been discovered. You select *Add the unregistered device to registered device* for the device in the *Unregistered Devices* list. For more information, see “Viewing unregistered devices (EMS mode)” on page 93.

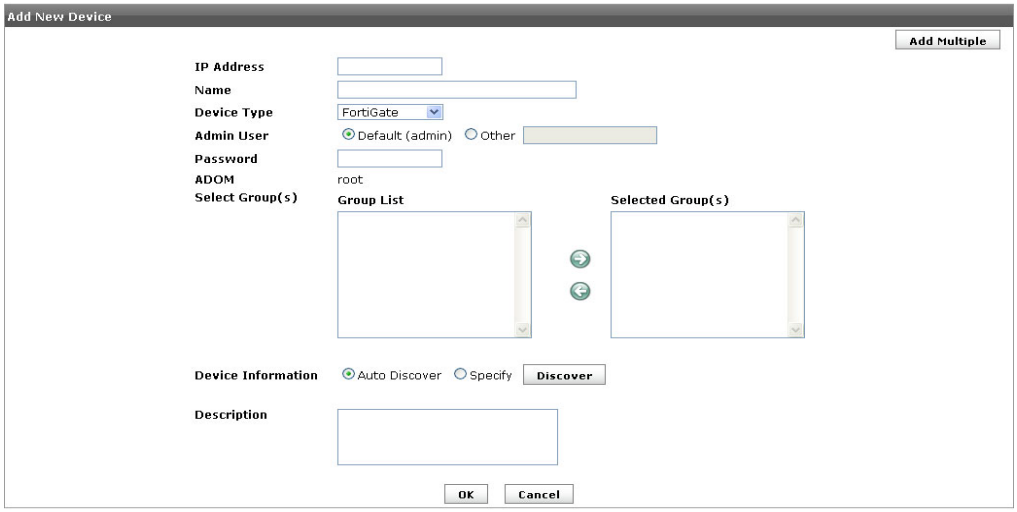
Adding an operating FortiGate HA cluster to the Device Manager is similar to adding a standalone device. For more information, see “Adding a FortiGate HA cluster” on page 96.

Once a device or group has been added to the Device Manager module, the configurations and information can be shared with other modules in the FortiManager system for proper management and control.

To add a device

1 From the Main Menu Bar, select *Add Device*.

Figure 46: Adding a device



2 In the *Add New Device* window, complete the following fields:

IP Address	Enter the IP Address of the device you want to add. The FortiManager system uses the IP address to find and retrieve the configuration data from the device.
Name	Enter a unique name for the device.
Device type	Select the type of device you want to add: FortiGate, FortiSwitch, FortiGate Carrier, FortiMail, or FortiAnalyzer.
Admin User	Select one of the following:
Default (admin)	Select if the device uses the default “admin” as its admin user. For more information, see “Configuring administration settings” on page 61.
Other	Select and then enter the admin user name if the device uses a different user name.
Password	Enter the administration password. This is the password used to log in to the administrator account on the device.
ADOM	Select the ADOM to which the device binds. For more information, see “Administrative Domains” on page 33.
Select Groups	Select the group(s) that you want this device to belong to from the *Group List* field and use the right-pointing arrow to move it to the *Selected Group(s)* field. All groups that you have created for the device type will display in the *Group List* field.
Device Information	Select one of the following:
Auto Discover	Select, then select *Discover* for the FortiManager system to search for the device.
Specify	Select to manually enter the searching parameters: **Firmware Version** **MR Build No.** - the Maintenance Release build number **Device Model** **SN** - Serial Number of the device **Hard Disk Installed** - presence of a hard disk on the device.
Discover	In combination with *Auto Discover*, select to search for the device. The discovered device information appears.
Description	Add any notes or comments you have for this device.

3 Select *OK* to add the device.

Replacing a managed device

By default, the managed devices are not locked to their serial numbers. This means that the FortiManager system can continue to manage a replaced device as long as you configure the device network settings and connect the device to the network.

Optionally, each managed device can be locked to its actual serial number. This feature can be enabled with the following CLI command:

```
config fmsystem admin setting
  set verify_serial_number enable
end
```

In this scenario, 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.

Note: You can only re-install a device that has a *Retrieve* button under the *Revision History* tab. For more information, see “To re-install the configuration” on page 86.

To change the serial number

1 Configure the new device's IP address, gateway, admin password, and SSH/HTTPS access, and connect it to the FortiManager system. For more information, consult your device’s documentation.

2 Record the host name of the old device.

3 Use the following CLI command to replace the serial number of the old device with that of the new device:

```
execute device replace <device-id> <dev-ser-no>
```

Where `<device-id>` is the host name of the old device and `<dev-ser-no>` is the serial number of the new device.

To re-install the configuration

1 In the *Device Manager* window, select *FortiGate, FortiMail, or FortiAnalyzer* in the Navigation Pane.

2 In the Content Pane, select a device’s name.

3 Select *Revision History* for that device in the *Navigation Pane.*

The FortiManager system retrieves the current configuration of the new device as a new revision.

4 If available, select the last configuration revision that was installed to the old device and select *Revert to this version*. If its not available, no revisions have been saved for this device and the configuration cannot be re-installed.

A new revision is added to the *Revision History*.

5 In the Main Menu Bar, select *Install* to install the new revision.

For more information, see “Installing Device Configurations” on page 277.

6 Change the serial number from that of the old device to that of the new device in the reverted configuration, using the preceding procedure.

Viewing the device summary

You can view the summary information of all added devices or any individual device.

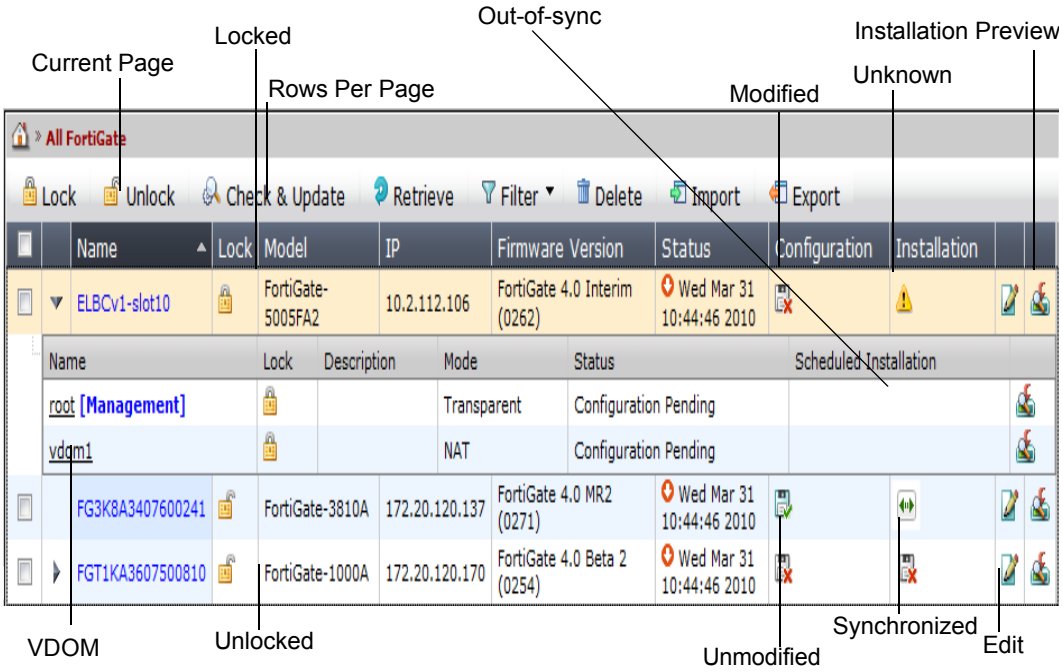
This section contains the following topics:

Viewing managed devices

In the Navigation Pane select *Device Manager* and the device type — Chassis, FortiGate, FortiMail, or FortiAnalyzer — to display that type of devices that are managed by the FortiManager system. You can then select a single device in the device tree to display a summary of all of the managed devices on one screen.

Selecting each column header sorts the information in ascending or descending order by that column. An arrow to the right of the column name indicates the currently selected column, and ascending (up arrow) or descending order (down arrow).

Figure 47: Sample FortiGate device list



Path	At the top left of the Content Pane, is a Home icon followed by the path to the location of the device you are viewing. For example if you are looking at a FortiGate unit with a host name of “myFortiGate” and VDOM called “vdom1” the path will display `Home icon>>All Fortigate >>myFortiGate>>vdom1.`
Lock	Select the check box beside a device that you want to lock, then select *Lock* to lock the device. This button appears only if you enable device locking. For more information, see “Device configuration locks” on page 69.

Unlock	Select the check box beside a device that you want to unlock, then select *Unlock* to unlock the device. This button appears only if you enable device locking. For more information, see “Device configuration locks” on page 69.
Check & Update	Refresh the connection between the selected devices and the FortiManager system. This operation updates the device status and the FortiGate HA cluster member information.
Retrieve	Select to synchronize the configuration running on the selected device with the device’s configuration file saved in the FortiManager repository.
Filter	Edit the column filters to filter or sort the device list according to the criteria you specify. For more information, see ““Adding filters to device list” on page 103”.
Delete	Select the check box beside a device that you want to delete, then select *Delete* to remove the device.
Import	Select to import large numbers of FortiGate units at once. For more information, see “Importing and exporting large numbers of devices” on page 97.
Export	Select to save a list of FortiGate units in a text file and import the file later as a backup. For more information, see “Importing and exporting large numbers of devices” on page 97.
Checkbox	Select one or more devices to apply an action to. Optionally select the checkbox at the top of the column to select all devices in the list. For example, select all and select Lock to lock all the devices.
Arrow	When displayed, select to expand device view to display the summary for the configured VDOMs. For more information, see “Configuring virtual domains (VDOMs)” on page 219.
VDOM	If a device has VDOMs, a blue arrow appears beside it. Select the arrow to display the VDOM summary. Select the VDOM name to view or edit the VDOM configuration. For more information, see “Configuring virtual domains (VDOMs)” on page 219.
Name	The name of a device.
Locked | Unlocked (icon)	Device locking status. You can lock or unlock a device by selecting the *Lock* or *Unlock* icon. This column appears only if you enable device locking. For more information, see “Device configuration locks” on page 69.
Model	The model of a device.
IP	The IP address of a device.
Firmware Version	The firmware product name, version number, and build number of a device.
Status	The status of the device and the time and date the status was last checked. A green arrow indicates the connection between a device and the FortiManager system is up. A red arrow indicates the connection is down.
Configuration	If all configurations on the device are saved as the latest revision in the FortiManager database, the *Modified* icon appears. Otherwise, the *Unmodified* icon appears.
Installation	If the configuration between the device and the FortiManager system is synchronized, a *Synchronized* icon with horizontal arrows appears. If the configuration between the device and the FortiManager system is not synchronized, an *Out-of-sync* icon with a red X appears. A yellow *Unknown* icon appears if the FortiManager system cannot detect which revision (in revision history) is currently running on the device. This is normally due to a change made on the device directly or connection error.

Edit icon	Edit device information. Editing the information for a device is not the same as editing the configuration settings. For information on modifying the configuration settings of a device, see “Configuring devices” on page 217.
Installation Preview icon	Select to display a set of commands that will be used in an actual device configuration installation in a new window.

Viewing all groups

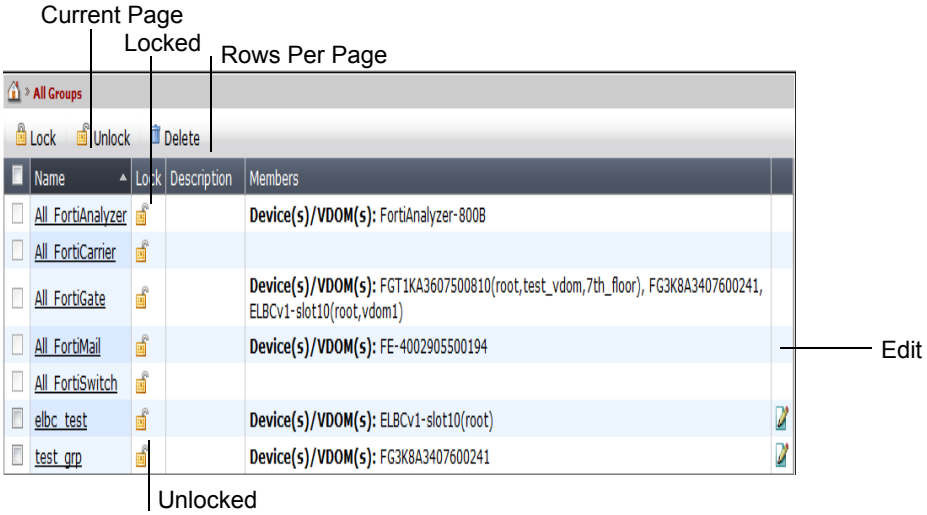
You can select *Device Manager* > *Group* in the Navigation Pane to view the device groups.

The five default groups (All FortiAnalyzer, All FortiCarrier, All FortiGate, All FortiMail, and All FortiSwitch) are generated by the FortiManager system and cannot be modified.

Selecting each column header sorts the information in ascending or descending order by that column. An arrow beside the column name indicates the currently selected column, and ascending or descending order.

You can create new groups that include any number of devices. See “Adding a device” on page 84.

Figure 48: All groups



Path	At the top left of the Content Pane, is a Home icon followed by the path to the location of the device you are viewing. For example if you are looking at a FortiGate unit with a host name of “myFortiGate” and VDOM called “vdom1” the path will display `Home icon>>All Fortigate >>myFortiGate>>vdom1.`
Lock	Select the check box beside a group that you want to lock, then select *Lock* to lock the group. This button appears only if you enable device locking. For more information, see “Device configuration locks” on page 69.
Unlock	Select the check box beside a group that you want to unlock, then select *Unlock* to unlock the group. This button appears only if you enable device locking. For more information, see “Device configuration locks” on page 69.
Delete	Select the check box beside a group that you want to delete, then select *Delete* to remove the group.
Checkbox	Select one or more groups. Optionally select the checkbox at the top of the column to select all custom groups in the list. Once selected, apply action to selected groups.

Name	The name of a group. *All FortiAnalyzer, All FortiCarrier, All FortiGate, All FortiMail*, and *All FortiSwitch* are default groups and cannot be edited or deleted.
Locked | Unlocked (icon)	Group locking status. You can lock or unlock a group by selecting the *Lock* or *Unlock* icon. This column appears only if you enable device locking. For more information, see "Device configuration locks" on page 69.
Description	Any notes or comments about a group.
Members	Members or groups included in a group.
Edit icon	Edit a group.

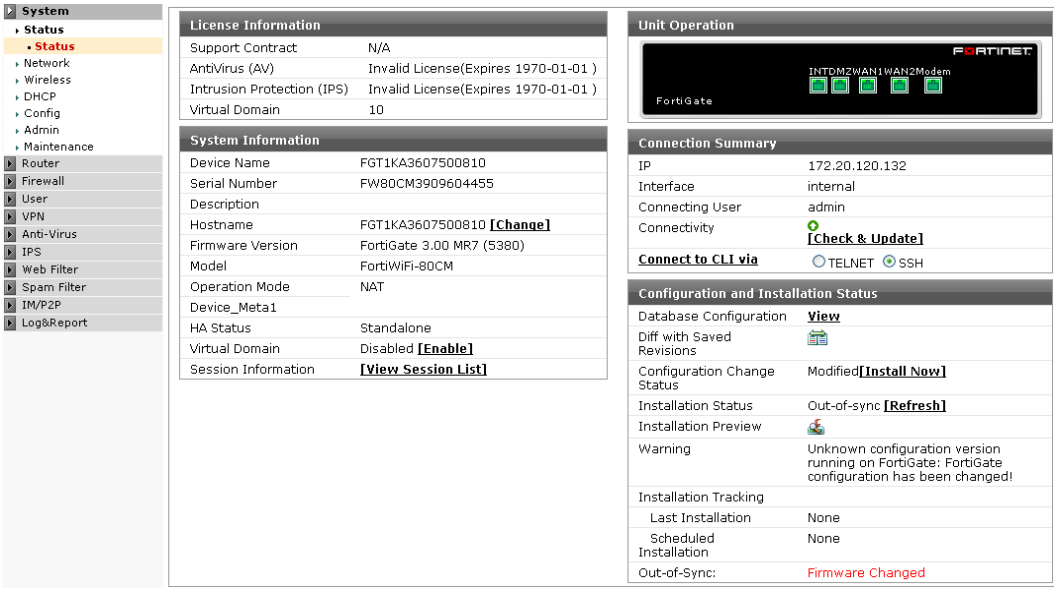
Viewing a single device

You can view information about individual devices in the FortiManager system. This section describes only the FortiGate unit summary because it has more summary items than the other devices. The other devices are similar.

To view a device, in the Navigation Pane, select *Device Manager* > *FortiGate*, and select a device in the Content Pane.

By default, the Navigation Pane will display the navigation options from that device — normally System, Router, Firewall, UTM, VPN, User, WAN Opt, Endpoint, and Log & Report. Refer to the *FortiGate CLI Reference* document for configuring the FortiGate devices as well as details of related fields. The Content Pane will display the status information for that device.

Figure 49: Example FortiGate unit summary



License Information

Support Contract	The support contract number and expiry date.
AntiVirus (AV)	The contract version, issue date and service status.
Intrusion Protection (IPS)	The contract version, issue date and service status.
Web Filtering	License type, expiry date and service status. GMS mode only.
AntiSpam	License type and expiry date and service status. GMS mode only.

Virtual Domain	The number of virtual domains that the device supports.
System Information	
Name	The name of the device.
Serial Number	The device serial number.
Description	Descriptive information about the device.
Hostname	The device hostname.
Firmware Version	The device firmware version and build number.
Model	The device model number.
Operation Mode	Operational mode of the FortiGate unit: NAT or Transparent.
HA Mode	Standalone indicates non-HA mode.
Virtual Domain	Enabled or disabled the device's virtual domains.
Unit Operation	An illustration of the FortiGate unit's front panel showing the unit's Ethernet network interfaces. For more information, see the *FortiGate Administration Guide*.
Connection Summary	
IP	The IP address of the device.
Interface	The port used to connect to the FortiManager system.
Connecting User	The user name for logging in to the device.
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 *Check Now* to test the connection between the device and the FortiManager system.
Configuration and Installation Status	
Database Configuration	Select *View* to display the configuration file of the FortiGate unit.
Diff with Saved Revisions	Select *Diff* icon to show only the changes or differences between the saved configuration revision and another revision. For more information, see "Comparing different configuration files" on page 280.
Configuration Change Status	One of the following: **Modified**: All configuration displayed on the device is saved as the latest revision in the FortiManager database. **Unmodified**: Some configuration on the device has changed since the latest revision in the FortiManager database. Select *Save Now* to install and save the configuration. For more information, see "Configuration" on page 88 and .
Installation Status	One of the following: **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. For more information, see "Installation" on page 88.
Installation preview	Select icon to display a set of commands that will be used in an actual device configuration installation in a new window.

Warning	One of the following: **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. **Aborted**: The FortiManager system cannot access the device.
Installation Tracking	One of the following: **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.
Out-of-Sync	This option appears when the version of the configuration saved on the FortiManager repository is different from the one on the device. You can retrieve the latest configuration. See “Retrieve” on page 92.

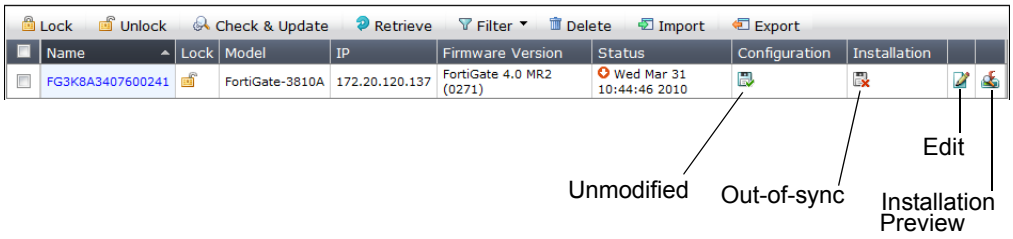
Viewing out-of-sync devices

You can view the devices of which the configurations are not synchronized with the FortiManager system. For information on how managed devices interact with the FortiManager system, see “Configuration and installation workflow” on page 18.

To view out-of-sync devices, select *Device Manager* > *Out-of-Sync Device* from the Navigation Pane.

Selecting each column header sorts the information in ascending or descending order by that column. An arrow beside the column name indicates the currently selected column, and ascending or descending order.

Figure 50: Out-of-sync device list



Lock	Select the check box beside a device that you want to lock, then select *Lock* to lock the device. This button appears only if you enable device locking. For more information, see “Device configuration locks” on page 69.
Unlock	Select the check box beside a device that you want to unlock, then select *Unlock* to unlock the device. This button appears only if you enable device locking. For more information, see “Device configuration locks” on page 69.
Check & Update	Refresh the connection between the selected devices and the FortiManager system. This operation updates the device status and the FortiGate HA cluster member information.
Retrieve	Select to synchronize the configuration running on the selected device with the device’s configuration file saved in the FortiManager repository.
Filter	Edit the column filters to filter or sort the device list according to the criteria you specify. For more information, see ““Adding filters to device list” on page 103”.
Delete	Select the check box beside a device that you want to delete, then select *Delete* to remove the device.

Import	Select to import out-of-sync devices. For more information, see “Importing and exporting large numbers of devices” on page 97.
Export	Select to save a list of out-of-sync devices in a text file and import the file later as a backup. For more information, see “Importing and exporting large numbers of devices” on page 97.
Checkbox	Select one or more devices to apply an action to. Optionally select the checkbox at the top of the column to select all devices in the list. For example, select all and select Lock to lock all the devices.
Name	The name of a device.
Locked | Unlocked (icon)	Device locking status. You can lock or unlock a device by selecting the *Lock* or *Unlock* icon. This column appears only if you enable device locking. For more information, see “Device configuration locks” on page 69.
Model	The model of a device.
IP	The IP address of a device.
Firmware Version	The firmware version number and build number of a device.
Status	The status of a device and the time and date the status was last checked. A green arrow means that the connection between a device and the FortiManager system is up; a red arrow means that this connection is down.
Configuration	If all configuration on the device is saved as the latest revision in the FortiManager database, the *Modified* icon appears. Otherwise, the *Unmodified* icon appears.
Installation	If the configuration between the device and the FortiManager system is synchronized, a *Synchronized* icon appears. If the configuration between the device and the FortiManager system is not synchronized, an *Out-of-sync* icon appears. An *Unknown* icon appears if the FortiManager system cannot detect which revision (in revision history) is currently running on the device. This is normally due to a change made on the device directly or connection error.
Edit icon	Edit device information. Editing the information for a device is not the same as editing the configuration settings. For information on modifying the configuration settings of a device, see “Configuring devices” on page 217.
Installation Preview icon	Select to display a set of commands that will be used in an actual device configuration installation in a new window.

Viewing unregistered devices (EMS mode)

Unregistered devices are

- devices that are configured through their web-based manager or CLI to be managed by this FortiManager system
- devices that have configured the FortiManager system as the AntiVirus and IPS Options override server
- devices that have configured the FortiManager system as the Webfilter/AntiSpam override server.

Depending on settings (see “Setting unregistered device options” on page 94), the FortiManager system can ignore unregistered devices, or it can add them to the *Unregistered Devices* list with or without FortiGuard service. A device is listed in this list when it first requests service.

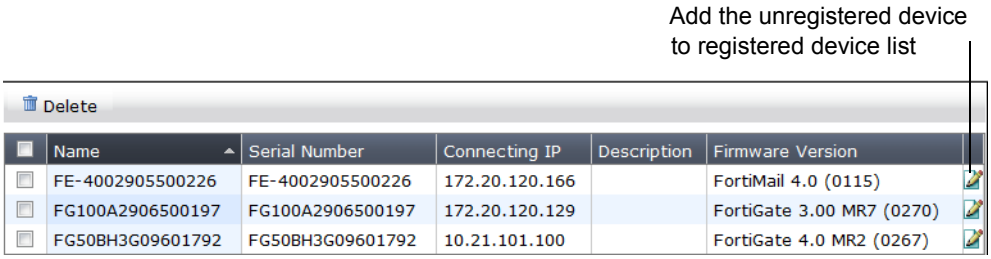
Optionally, you can select devices from the *Unregistered Devices* list and make them managed devices.

Caution: Do not leave an HA cluster in the *Unregistered Devices* list. HA failover can cause disruption to services. Add the cluster as a managed device.

To view unregistered devices, select *Device Manager* > *Unregistered Device* from the Navigation Pane.

Clicking the column header *Name* or *Connecting IP* sorts the information in ascending or descending order by that column. An arrow beside the column name indicates the currently selected column, and ascending or descending order.

Figure 51: Unregistered devices list

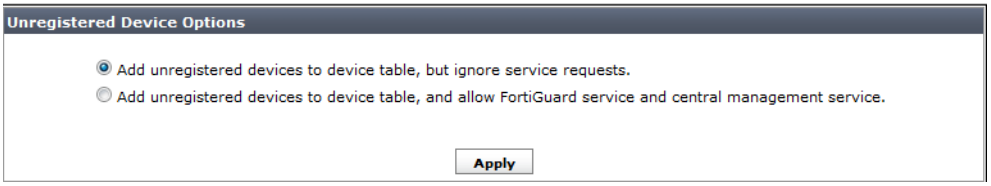


Delete	Select the check box beside a device that you want to delete, then select *Delete* to remove the device.
Checkbox	Select one or more devices to apply an action to. Optionally select the checkbox at the top of the column to select all devices in the list. For example, select all and select Lock to lock all the devices.
Name	Device (host) name.
Serial Number	Device serial number
Connecting IP	The IP address used to connect to the unregistered device.
Description	Any notes or comments on the device.
Firmware Version	The firmware revision running on the device.
Edit icon	Edit the status of this device to add the device to the managed devices list. For more information, see “Adding a device” on page 84.

Setting unregistered device options

To choose how FortiManager system handles unregistered devices, from the Navigation Pane, select *Device Manager* > *Unregistered Device* > *Unregistered Devices Options* (EMS Mode only).

Figure 52: Unregistered devices options



Add unregistered devices to device table, but ignore service requests	Unregistered devices are automatically added to the *Unregistered Devices* list, but cannot receive FortiGuard updates.
Add unregistered devices to device table, and allow FortiGuard service and central management service	Unregistered devices are automatically added to the *Unregistered Devices* list and subscribers to the FortiGuard service can receive updates. For information on configuring to receive updates, see "Using FortiGuard services" on page 249.
Apply	Select to save the setting.

Deleting devices

You can delete devices from the FortiManager system. If the device exists in device groups, it will be removed from all device groups as well.

To delete devices

1. In the *Navigation Pane*, select *Device Manager* and type of device.
2. In the Content Pane, select the checkbox for the device or devices to be deleted.
3. Select *Delete*.

Adding FortiGate groups

You may want to divide the managed FortiGate units into groups for the following reasons:

- to configure group-shared settings and then install the configurations on the units all at once
- to group the units according to their locations or ownership
- to manage a great number of units more efficiently.

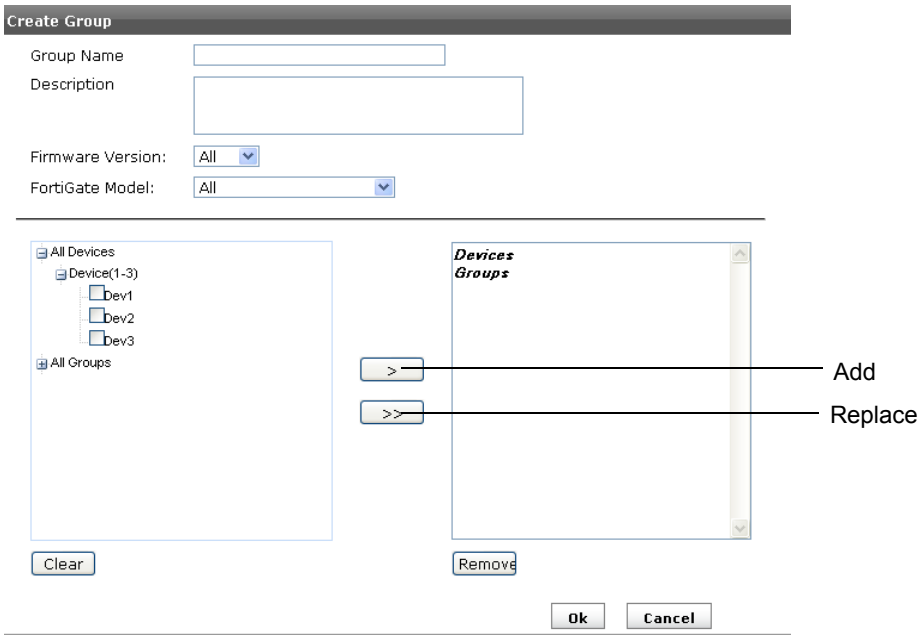
You can also create FortiGate groups that contain virtual domains.

This section contains the following topics:

Adding a FortiGate group

To add a group, select *Add Group* from the Main Menu Bar.

Figure 53: Adding a FortiGate group



Group Name	Enter a unique group name (maximum 16 characters). The name cannot be the same as the name of another device or device group.
Description	Enter a description for the FortiGate group. You can use the description to provide more information about the FortiGate group, such as its location.
Firmware Version	Select a firmware version for the group. All members of the group must run this firmware version.
FortiGate Model	Select a FortiGate model.
Add icon	Move the selected device from the device list to the group member list.
Replace icon	Replace one or more devices in the group member list with selected ones in the device list.
Clear	Clear the selections in the device list.
Remove	Clear the selected devices in the group member list.

Adding a FortiGate HA cluster

If you add an operating FortiGate High Availability (HA) cluster to the FortiManager system, make sure the server can access the cluster management interface through SSH and HTTPS. Then follow the procedures described in “Adding a device” on page 84.

You can also configure two standalone FortiGate units into one HA cluster.

Note: The *Lock* column appears in the device summary when device locking is enabled. Before you can make any configuration changes to a device, you must lock the device to avoid configuration conflicts with other administrators. For more information, see “Device configuration locks” on page 69.

To add two standalone FortiGate units into one HA cluster

1 Add the two units to the FortiManager system. For more information, see “Adding a device” on page 84.

2 Configure the two units into HA mode. One of them becomes the HA primary unit and the other one becomes the subordinate unit. For more information, see the *FortiGate Administration Guide*.

3 Delete the subordinate device from the FortiManager system device list.

Note: If the two FortiGate units are running in transparent mode, you must disable `arpforward` on the connection interfaces ***before*** you connect them into the network. Otherwise, arp loop traffic will cause network problems.

Viewing the device group summary

By selecting a group name in *Device Manager* > *Group*, you can view the group information you entered when adding the group (see "Adding FortiGate groups" on page 95), including the group membership and the configuration status of each member under this group.

Importing and exporting large numbers of devices

You can use the device *Import* feature to import large numbers of devices, ADOMs, device VDOMs, and device groups at once. You can use the device *Export* feature to save a list of devices in a text file as a backup and import the file later.

This section contains the following topics:

Text file format

Before you can import new devices for the first time, you must have a text file that contains information about the devices to be imported. The first line of the file specifies the version of the format and is the same for every type of devices:

```
device_list_ver=6
```

Following this line are a number of lines describing ADOMs, devices, device VDOMs, and device groups. Blank lines and lines beginning with '#' as the first character are ignored. These lines are for users to add comments when import devices. In addition, each entry in the file must span only a single line. No entries can span multiple lines. Disable the text wrapping feature of your text editor.

Device file format

Devices are specified by the following device lines:

```
device_list_ver=6
device|ip|name|platform|user|passwd|adom|desc|discover|reload|
   |fmver|mr|sn|has_hd|
```

The fields after "reload" are optional, and only need to be provided if discover is set to 0. The list in the text file should contain the following fields:

Field Name	Blank Allowed	Description
ip	No	Device IP address.

platform	No	The device type. For example, FortiGate, or the full platform name: FortiWifi-60B.
user	No	Admin username.
passwd	Yes	Admin password.
adom	Yes	The ADOM into which this device should be imported. If this field is left blank, the device is imported into the current ADOM.
desc	Yes	Device description.
discover	No	Enter 1 to automatically discover device, 0 otherwise.
reload	No	Enter 1 to reload the device configuration after importing it, 0 otherwise.
fwver	No	Firmware version. Currently supported: 3.00 and 4.00.
mr	No	MR designation of the device. For example, GA, MR1, MR2.
sn	No	Device serial number.
has_ha	No	Enter 1 if the device has a hard disk, 0 if not.

Following the device line, there may be one or more “+meta” lines specifying metadata for the device (For more information, see “Metadata file format” on page 99), or one or more “+vdom” lines specifying device VDOMs.

VDOMs are specified by the following lines:

```
+member|devname|vdom|
+subgroup|groupname|
```

Field Name	Blank Allowed	Description
devname	No	Name of the device.
vdom	Yes	The VDOM of the device that belongs to this group. If this field is left empty, the VDOM refers to the root VDOM.
groupname	No	The name of the subgroup that belongs to this group. Note that only 2 levels of group nestings are permitted in FortiManager 4.0.

ADOM file format

ADOMs are specified by the following ADOM lines:

```
device_list_ver=6
adom|name|mode|enable|
```

One or more “+meta” lines may follow a ADOM line to specify the values of metadata associated with that ADOM. See “Metadata file format” on page 99.

Field Name	Blank Allowed	Description
Name	No	Name of the ADOM.
Mode	No	EMS or GMS.
Enable	No	Enter 1 to enable, 0 to disable.

Group file format

Device group are specified as follows:

```
device_list_ver=6
group|name|desc|adom|
```

Field Name	Blank Allowed	Description
Name	No	Name of the group.

desc	No	Group description.
adom	Yes	The ADOM to which the group belongs. If the field is left blank, it refers to the ADOM from which the import operation is initiated.

One or more “+meta” lines describing metadata values for the group, or one or more lines describing group members and subgroups, may follow the group line. See see “Metadata file format” on page 99.

```
+member|devname|vdom|
+subgroup|groupname|
```

Field Name	Blank Allowed	Description
devname	No	Name of the device.
vdom	Yes	The VDOM of the device that belongs to this group. If this field is left empty, the VDOM refers to the root VDOM.
groupname	No	The name of the subgroup that belongs to this group. Only 2 levels of group nestings are permitted in FortiManager 4.0.

Metadata file format

ADOMs, devices, and groups may have metadata associated with them. Their values are specified by +meta lines following the device, group, or ADOM. You can use multiple lines to specify multiple metadata values.

```
+meta|name|value|
```

Field Name	Blank Allowed	Description
name	No	The name of the metadata.
value	No	The associated value.

String transliterations

Certain fields, such as the description fields and metadata value fields, may contain characters with special meaning in this file format. In order to safely represent these characters, the following transliteration scheme is used:

Character	Transliteration
newline	\n
carriage return	\r
tab	\t
|	\!
****	\\
non-printable character	\xAA where AA is a two-digit hexadecimal number representing the byte value of the character.

Example text files

Here are three examples of what a text file might look like. For more information, see “Text file format” on page 97.

Example 1: Device

```
device_list_ver=7
# Device definitions. The lines beginning with '+' are
# associated with the device, and will cause an error if they
# appear out-of-context.

device|10.0.0.74|top|FortiGate|admin||root|My description.|1|1|
```

```
+meta|bogosity|10|
+vdom|vdom01|root|
+vdom|vdom02|root|
+vdom|vdom03|root|
+vdom|vdom04|root|

device|10.0.0.75|bottom|FortiGate-
   400A|admin|password|adom01|Your
   description.|0|1|3.00|MR6|FG400A2905550018|0|
+meta|bogosity|12|
+vdom|vdom01|adom01|
```

Example 2: ADOM

```
device_list_ver=7
# ADOM definitions. These are exported only from the root ADOM,
# and can only be imported in the root ADOM. Import will abort
# with an error if this is imported in a non-root ADOM.
# The lines beginning with '+' are associated with the
# last-defined ADOM, and will cause an error if they appear
# out-of-context.

adom|root|GMS|1|
+meta|tag|my domain|

adom|adom01|EMS|1|
+meta|tag|your domain|
```

Example 3: Device group

```
device_list_ver=7
# Group definitions. Groups will be created in the order they
# appear here, so subgroups must be defined first,followed by
# top-level groups. Only two levels of nesting are supported.

group|group01|My description.|root|
+member|bottom||
+member|top|vdom03|

group|group02|Another description.|root|
+meta|supervisor|Joe S. H. Moe|
+member|top|vdom01|
+member|top|vdom02|
+subgroup|group01|

group|group03||adom01|
+meta|supervisor|Anne O. Nymous|
```

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

Device import work flow

When you import devices, the FortiManager system first checks the text file for each device. There are only two possible outcomes:

- If the text file is complete and correct, the device will be added, regardless of any other settings in the file. See “Device discovery flow chart” on page 101 and “Device resync flow chart” on page 102 for more details.
- If the text file is not correct or is incomplete, the results will depend on the Discovery and Retrieve outcome. See “Device discovery flow chart” on page 101 and “Device resync flow chart” on page 102 for more details.

Figure 54: Device discovery flow chart

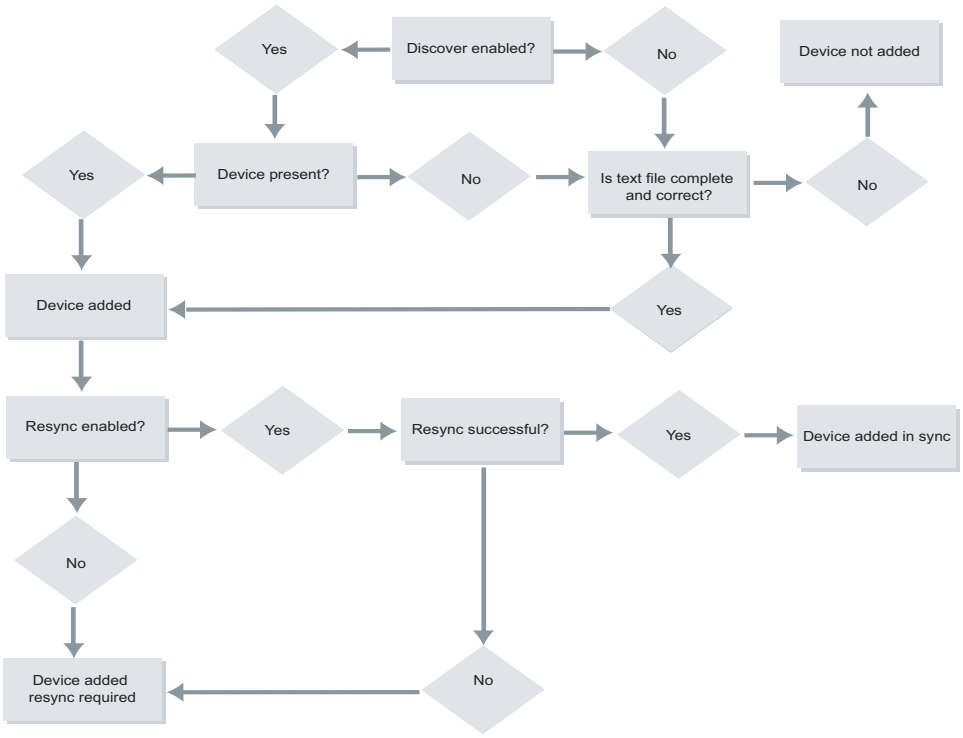
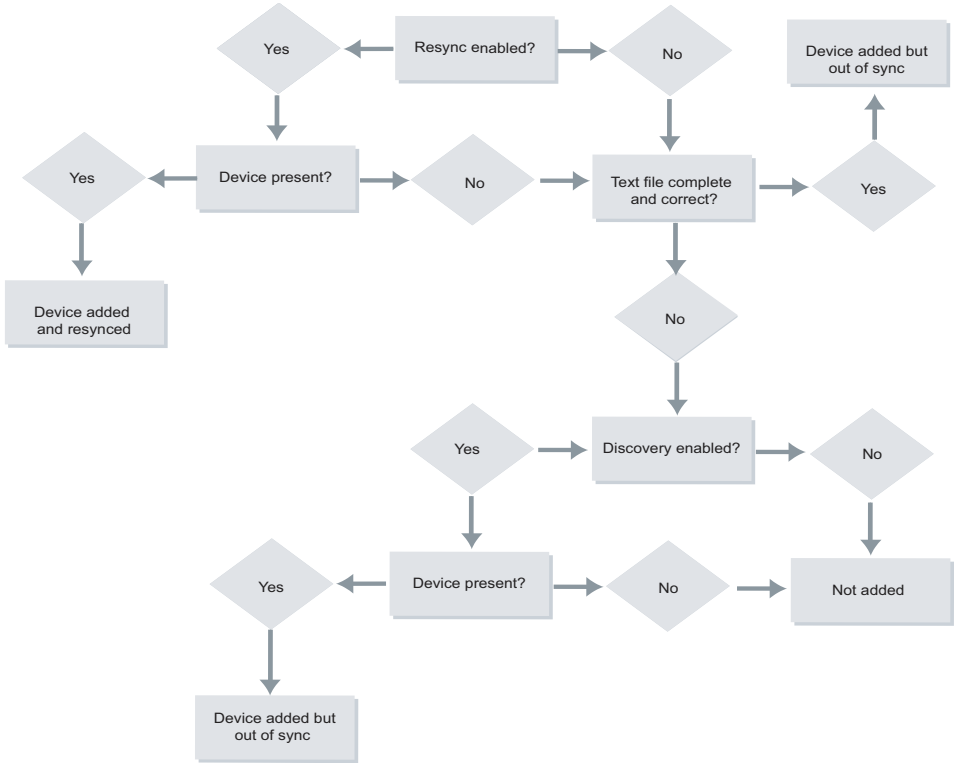


Figure 55: Device resync flow chart



Note: Device information acquired through the Discovery or Retrieve features will replace the device information contained in the text file.

Importing and exporting devices

There are two ways to get the text file:

- Use a backup file.
- Create it manually. For more information, see “Text file format” on page 97.

When you select *Export* in the Main Menu Bar, it does not actually remove the devices from the FortiManager system. A list of devices is saved to the location you specified. It can be used as a backup file and imported later.

The exported list contains the full device details.

To bulk import devices

1 In the Navigation Pane, select *Devices* > *Device*.

2 In the Content Pane, select *Import*.

3 Select *Browse* and locate and specify the device list text file.

4 Select *Submit*.

To bulk export devices

1 In the Navigation Pane, select *Device Manager* and type of device.

2 In the Content Pane, select *Export*.

3 Save the file.

Adding filters to device list

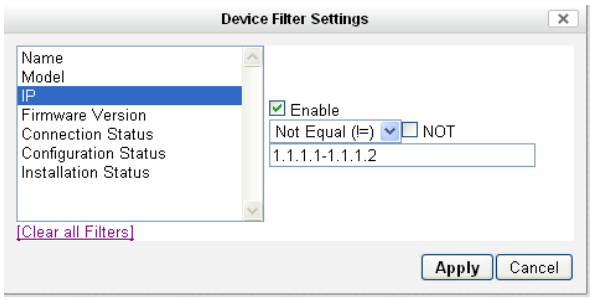
You can add filters to control the information that is displayed by the device list. Filters are useful for reducing the number of entries that are displayed on a list so that you can focus on the information that is important to you.

You add filters to a device list by selecting *Devices* > *Device* in the Navigation Pane, then the *Filter* button in the Content Pane to display the *Device Filter Settings* window. From this window, you can select any column name to filter, and configure the filter for that column. You can also add filters for one or more columns at a time.

Filters for columns that contain numbers

If the column includes numbers (for example, *IP* addresses) you can filter by a single number or a range of numbers. For example, you could configure a device IP column to display only entries for a single IP address or for all IPs in a range. To specify a range, separate the top and bottom values of the range with a hyphen, for example 25-50.

Figure 56: A device list filter set to display devices with IP address in the range of 1.1.1.1-1.1.1.2

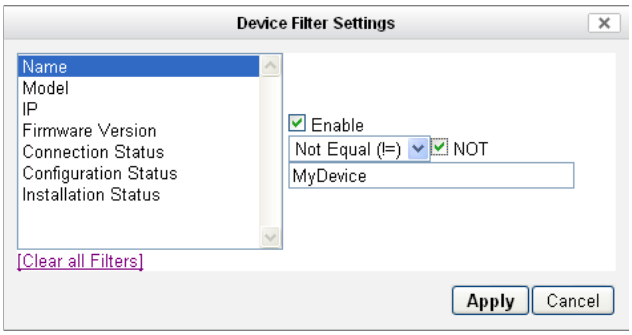


Filters for columns containing text strings

If the column includes text strings (for example, *Name*) you can filter by a text string. You can also filter information that is an exact match for the text string (equals), that contains the text string, or that does not equal or does not contain the text string.

The text string can be blank and it can also be very long. The text string can also contain special characters such as `<`, `&`, `>` and so on. However, filtering ignores characters following a < unless the `<` is followed by a space (for example, filtering ignores `<string` but not `< string`). Filtering also ignores matched opening and closing `<` and `>` characters and any characters inside them (for example, filtering ignores `<string>` but does not ignore `>string>`).

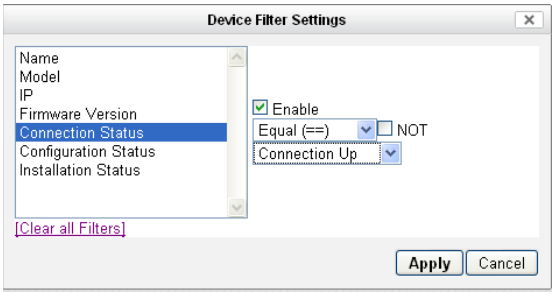
Figure 57: A device list filter set to display all devices but one named “MyDevice”



Filters for columns that can contain only specific items

For columns that can contain only specific items (for example, *Model* and *Connection Status*), you can select a single item from a list.

Figure 58: A device list filter set to display all devices with Connection Status set to "Connection Up"



Using the CLI console for managed devices

You can access the CLI commands of the managed devices by selecting *Terminal* from the Main Menu Bar. To use the CLI, you connect via Telnet or SSH.

Note: To connect to a device using Telnet or SSH, those methods of access must be enabled on the interface of the device connected to the FortiManager system. If they are not enabled, go the device and enable them before connecting via CLI.

Figure 59: CLI Console

Connect to	Select the device that you want to access through the CLI. Alternatively, you can select *Specify* and enter the device's IP address.
TELNET | SSH	Select one of these programs used by the FortiManager system to open the CLI console.
Connect | Disconnect	Connect to the device you select, or terminate the connection.
Close	Exit the CLI console.

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

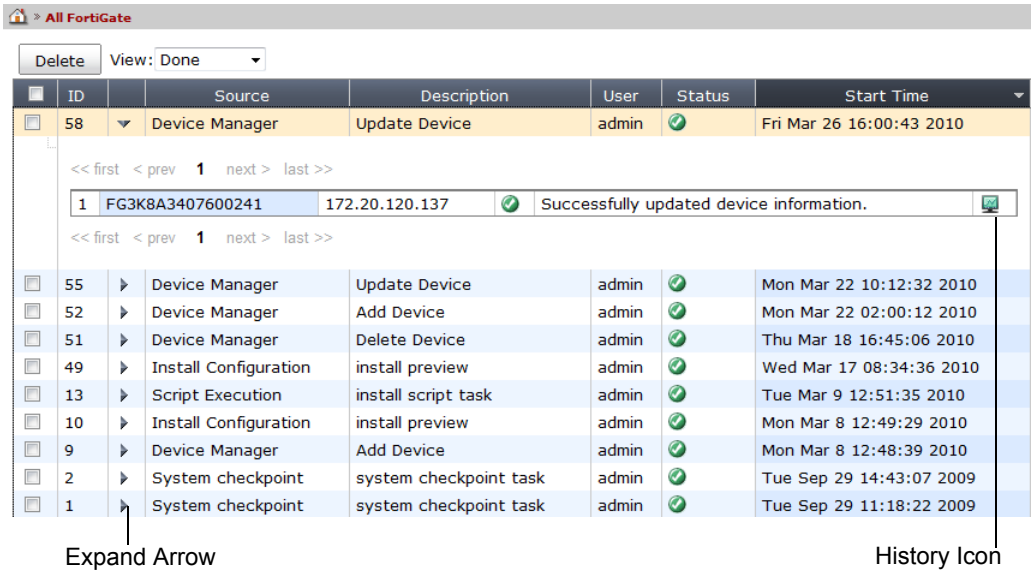
Using the task monitor

Using the task monitor, you can view the status of the tasks that you have performed.

From the Main Menu Bar, select *Task Monitor*. Select the *All FortiGate, All FortiSwitch*, or *All FortiAnalyzer* tab in the Navigation Pane, then in the Content Pane select a task categoryin the*View* field.

Clicking a column header sorts information in ascending or descending order by that column. An arrow to the right of the column name indicates the currently selected sorting column, and if it is ascending (up arrow) or descending (down arrow) order.

Figure 60: Viewing task list



Delete	Remove a selected task in the list.
View	Select the task status to view from the drop down menu. Status includes Running, Done, Error, Cancelling, Cancelled, Aborting, Aborted, and All.
Checkbox	Select one or more entries to apply an action to. Optionally select the checkbox at the top of the column to select all entries in the list.
ID	The identification number for a task.
Expand arrow	Select to display the specific actions taken under this task. When viewing the specific actions taken, the list will include the device it was run on, the device's IP address, an icon and message sayng if the task was successful, and a history icon you can select for task history for this device.
Source	The platform from where the task is performed.
Description	The nature of the task.
User	The users who have performed the tasks.
Status	Status of task: **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 the task started.

Searching for global objects

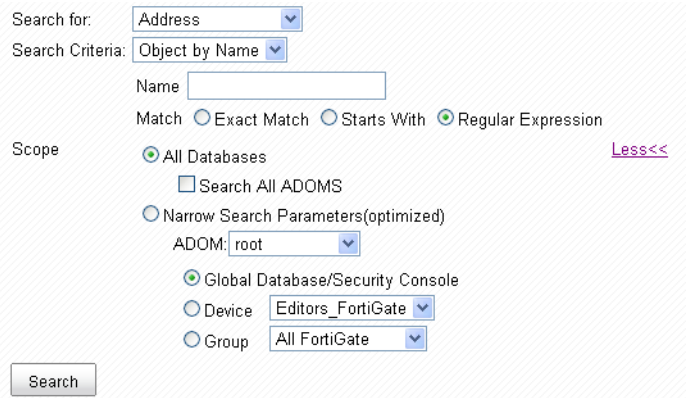
You can search the FortiManager system databases for different types of global objects based on the object input or usage.

Currently, you can search for the following global objects:

- address
- address group
- service
- service group
- protection profiles

To search, select *Search* from the Main Menu Bar. On the search screen, enter the following information.

Figure 61: Searching the databases



Search for	Select the global object that you want to search.
Search Criteria	Select the value upon which the search is based: • *Object by Name:* This option is available for all object types in the *Search for* field. If you select this option, enter the object name and select a matching method: ***Exact Match***: Select to require that matching object must be the same as the object name entered. This is case sensitive. If an object name does not match the object name entered, it will not be included in the search results. ***Starts With***: Select to require that matching object must start with a letter (case sensitive) or word at the beginning of the object name entered. For example, you can enter A to search for Addr1. ***Regular Expression***: Select to search with wildcards or Perl regular expressions. See http://perldoc.perl.org/perlretut.html for detailed information about using Perl regular expressions. • *Object by Value:* This option is available only when you select *Address* or *Service* in the *Search for* field. If you select *Address* in the *Search for* field and then *Object by Value* in the *Search Criteria* field, select the value type (*IP Address/Range* or *FQDN*) and enter the IP or FQDN in the *Address* field. You can use the exact match or regular expression to enter the IP or FQDN. For information on IP search rules, see "IP address search rules" on page 107. For information on firewall addresses, see "Address" on page 123. If you select *Service* in the *Search for* field and then *Object by Value* in the *Search Criteria* field, select a protocol and enter the corresponding information for the protocol. For more information, see "Service" on page 123. • *Unused Objects*: This option is available for all object types in the *Search for* field. This option is typically used by system administrators on a periodic basis to clean up the system. Over time, more and more objects are added to the system and then removed from policies or other uses. However, they still exist in the FortiGate configuration. There are no additional search parameters required for this option. • *Object usage*: This option is available for all object types in the *Search for* field. This option is typically used by system administrators to identify where an object is being used, that is, which policy or device is using it. There are no additional search parameters required for this option.
Scope	Specify the search scope for an object. To access additional scope information, including *Search All ADOMs* and *Narrow Search Parameters* options, select *more* >>. To hide these options select << *Less.* When you select *Object by Name, Object by Value, or Unused Objects* in the *Search Criteria* field, after entering the search criteria, you can search an object globally or narrow the search by selecting an ADOM. • *All Databases*: Select to search all databases in the FortiManager system. You can also select *Search All ADOMS* to search the databases of each ADOM. • *Narrow Search Parameters (optimized)*: If you know which ADOM the object is in, select this option to save search time. You can select the *ADOM*, the *Global Database*/*Security Console* of the ADOM, or a particular *Device* or *Group* of the ADOM. For more information, see "To search an object by name" on page 108, "To search an object by value" on page 109, and "To search a unused object" on page 110. When you select *Object Usage* in the *Search Criteria* field, you can find out where an object is being used, that is, which policy or which device is using it. For more information, see "To search an object by usage" on page 111.

IP address search rules

If you select *Address* in the *Search for* field and then *Object by Value* in the *Search Criteria* field, select the value type (*IP Address/Range* or *FQDN*) and enter the IP or FQDN in the *Address* field. You can use the exact match or regular expression to enter the IP or FQDN.

The following examples explain the IP address search rules.

Assuming that we have the following IP address definitions:

#	IP Address/Mask or IP Range
1	192.169.10.1/32
2	192.169.10.0/24
3	192.169.0.0/16
4	192.169.10.1-192.169.10.9
5	192.169.10.10-192.169.10.19

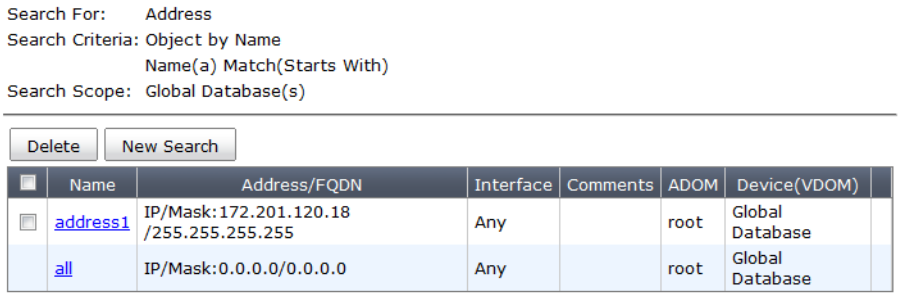
- If you enter an IP/mask or IP range, the search result will be an exact match of the value you entered.
  For example, searching 192.169.10.1/32 returns IP #1 in the table and searching 192.169.10.1-192.169.10.9 returns IP #4 in the table.
- If you enter a single IP, all definitions that include the IP in its range will be displayed.
  For example, searching 192.169.10.2 returns #2, 3, and 4 in the table, and searching 192.169.10.20 returns #2 and 3 in the table.
- If you enter an IP wildcard, all definitions within the subnet will be displayed.
  For example, searching 192.169.10.* returns #1, 2, 4, and 5 in the table, and searching 192.169.*.* returns #1, 2, 3, 4, and 5 in the table.

To search an object by name

1. From the Main Menu Bar, select *Search*.
2. In the *Search for* field, select an object.
3. In the *Search Criteria* field, select *Object Name.*
4. Enter the object name, then select a search method.
5. In the *Scope* field, select global database or a particular device/device group within which to search for the object. You can select *More>>* to add more search parameters:
   - *All Databases*: Select to search all databases in the FortiManager system. You can also select *Search All ADOMS* to search the databases of each ADOM.
   - *Narrow Search Parameters (optimized)*: If you know which ADOM the object is in, select this option to save search time. You can select the *ADOM*, the *Global Database*/*Security Console* of the ADOM, or a particular *Device* or *Group* in the ADOM.
6. Select *Search*.

   The search result displays.

Figure 62: Example search result for addresses



Delete	Select the check box beside an address that you want to delete, then select *Delete* to remove it. If there is no checkbox beside an address, it means that this address is used by an address group.
New Search	Select to start a new search.
Name	The name of an address.
Address/FQDN	The IP address/mask of the address.
Detail	Any comments added for the firewall address.
ADOM	The administrative domain that this address is in. For information about ADOM, see "Administrative Domains" on page 33.
Device (VDOM)	The database where this address is saved.
Filter	Display the devices and groups that can use the global firewall address configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Configuring firewall address groups" on page 133.

To search an object by value

1 From the Main Menu Bar, select *Search*.

2 In the *Search for* field, select *Address* or *Service*.

3 In the *Search Criteria* field, select *Object by Value.*

4 Do one of the following:

- If you selected *Address* in the *Search for* field, select the value type (*IP Address/Range* or *FQDN*) and enter the IP or FQDN in the *Address* field. You can use the exact match or regular expression to enter the IP or FQDN. For more information about address, see "Address" on page 123.
- If you selected *Service* in the *Search for* field, select a protocol and enter the corresponding information for the protocol following the table. For more information about service, see "Service" on page 123.

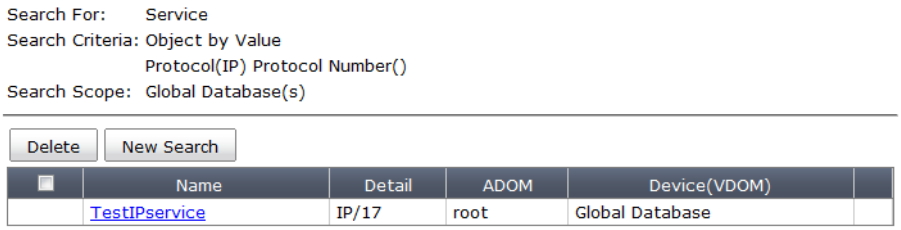
Protocol	Corresponding information
IP	Protocol Number: The IP protocol number for the service.
ICMP	Type: The ICMP type number for the service. Code: The ICMP code number for the service.
TCP/UDP	TCP Port Range: The TCP port number range. UDP Port Range: The UDP port number range.

5 Repeat step 5 in "To search an object by name" on page 108.

6 Select *Search*.

The search result displays.

Figure 63: Example search result for firewall services



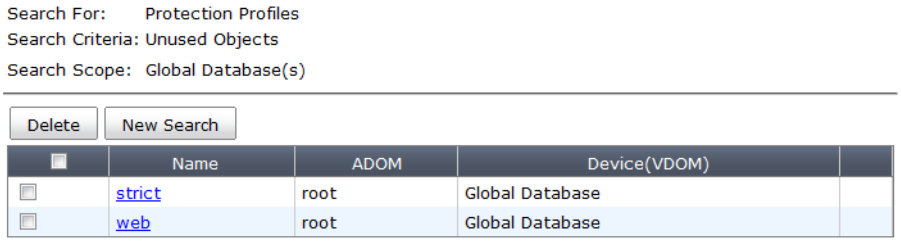
Delete	Select the check box beside a service that you want to delete, then select *Delete* to remove it. If there is no checkbox beside a service, it means that this service is used by a service group.
New Search	Select to start a new search.
Service Name	The name of the firewall service.
Detail	The protocol and port numbers for each service.
ADOM	The administrative domain that this service is in. For information about ADOM, see "Administrative Domains" on page 33.
Device (VDOM)	The database where this service is saved.
Filter	Display the devices and groups that can use the global firewall service configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration.

To search a unused object

1. From the Main Menu Bar, select *Search*.
2. In the *Search for* field, select an object.
3. In the *Search Criteria* field, select *Unused Objects*.
4. Repeat step 5 in "To search an object by name" on page 108.
5. Select *Search*.

   The search result displays.

Figure 64: Example search result for protection profiles



Delete	Select the check box beside a profile that you want to delete, then select *Delete* to remove it. If there is no checkbox beside a profile, it means that this profile is used by a firewall policy.
New Search	Select to start a new search.
Name	The name of the protection profile.

ADOM	The administrative domain that this service is in. For information about ADOM, see "Administrative Domains" on page 33.
Device (VDOM)	The database where this profile is saved.
Filter	Display the devices and groups that can use the global protection profile configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Configuring global antivirus file pattern" on page 137.

To search an object by usage

1. From the Main Menu Bar, select *Search*.
2. In the *Search for* field, select an object.
3. In the *Search Criteria* field, select *Object Usage*.
4. For *Scope*, do one of the following:
   - If you want to query where an object is used within the global database, select *Global Objects* and the object name that you want to search.
   - If you want to query which other device uses an object, select *Device Objects* and then a device containing the object and the object itself.
5. Select *Search*.

   The search result displays.

Figure 65: Example search result for firewall addresses

Search For: Address
Search Criteria: Object Usage
Search Scope: Global Objects(exampleAddress)

New Search

ADOM	Device(VDOM)	Referrer Type	Entry	Field
root	Global Database	firewall addrgrp	Internal_networks	member

New Search	Select to start a new search.
ADOM	The administrative domain that this address is in. For information about ADOM, see "Administrative Domains" on page 33.
Device (VDOM)	The database where this address is saved.
Referrer Type	The type of object that uses this address. In this case, the type is firewall address groups.
Entry	The name of the firewall address group that uses this address.
Field	The nature of the address in the address group, such as being added as a group member.

Configuring scripts

FortiManager scripts enable you to create, execute and view the results of scripts run on FortiGate devices attached to the FortiManager system. At least one FortiGate device must be configured on the FortiManager system for you to be able to use scripts.

To work with scripts, go to *Device Manager* > *Scripts*.

For more information, see “Working with Scripts” on page 223.

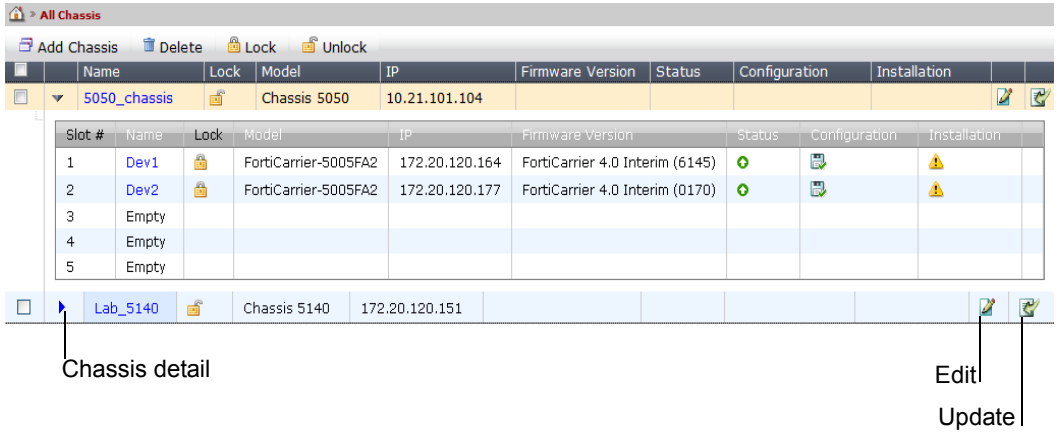
Working with Shelf Manager

The FortiManager system can work with Shelf Manager to manage the FortiGate-5050 and FortiGate-5140 chassis. The Shelf Manager runs on the Shelf Management Mezzanine hardware platform included with the FortiGate-5050 and FortiGate-5140 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 chassis and Shelf manager, go to http://docs.forticare.com/fgt5k.html.

You need to enable chassis management before you can work with the Shelf Manager through the FortiManager system. For information on enabling chassis management, see “Advanced settings” on page 77.

To view the chassis list, go to *Device Manager* > *Chassis*.

Figure 66: Chassis list



Breadcrumbs	Displays navigation history by showing sequence of selections made from the top level list to the current display. Select any step along the navigation history to display that level of detail. See “Breadcrumbs” on page 82.
Add Chassis	Select to add a new chassis. For more information, see “To add a chassis” on page 113.
Delete	Select the check box beside a chassis that you want to delete, then select *Delete* to remove it.
Lock (button)	Select the check box beside a chassis that you want to lock, then select *Lock* to lock the device. This button appears only if you enable device locking. For more information, see “Device configuration locks” on page 69.
Unlock (button)	Select the check box beside a chassis that you want to unlock, then select *Unlock* to unlock the chassis. This button appears only if you enable device locking. For more information, see “Device configuration locks” on page 69.
Chassis detail (button)	Select to display the FortiGate-5000 series blades contained in the chassis slots. For more information about the FortiGate blades list, see “Viewing the device summary” on page 87.
Name	Select the name of the chassis to display the blades in that chassis. See “Viewing the status of the FortiGate blades” on page 114.

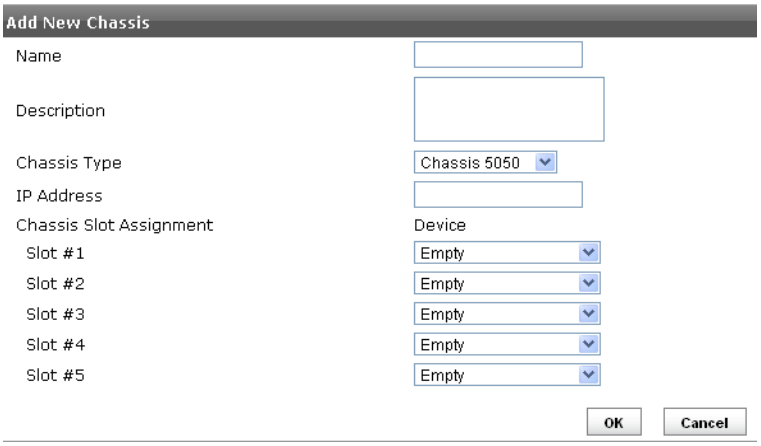
Locked | Unlocked (icon)	Device locking status. You can lock or unlock a device by selecting the *Lock* or *Unlock* icon. This column appears only if you enable device locking. For more information, see "Device configuration locks" on page 69.
Model	The model of a chassis.
IP	The IP address of the Shelf Manager running on the chassis.
Firmware Version	The firmware version number and build number of the Shelf Manager running on the chassis.
Status	The status of a Shelf Manager and the time and date the status was last checked. A green arrow means that the connection between a Shelf Manager and the FortiManager system is up; a red arrow means that this connection is down.
Configuration	If all configuration on the Shelf Manager is saved as the latest revision in the FortiManager database, the *Modified* icon appears. Otherwise, the *Unmodified* icon appears.
Installation	If the configuration between the Shelf Manager and the FortiManager system is synchronized, a *Synchronized* icon appears. If the configuration between the Shelf Manager and the FortiManager system is not synchronized, an *Out-of-sync* icon appears. An *Unknown* icon appears if the FortiManager system cannot detect which revision (in revision history) is currently running on the Shelf Manager. This is normally due to a change made on the Shelf Manager directly or connection error.
Edit icon	Edit chassis information and assign FortiGate-5000 series blades to the slots. For information, see "To edit a chassis and assign FortiGate-5000 series blade to the slots" on page 114.
Update icon	Select to refresh the connection between a Shelf Manager and the FortiManager system. You must lock the chassis before this operation.

To add a chassis

1 In the Navigation Pane, go to *Device Manager* > *Chassis*.

2 In the Content Pane, select *Add Chassis* and complete the following:

Figure 67: Adding a chassis



Name	Enter a unique name for the chassis.
Description	Optionally, enter any comments or notes about this chassis.
Chassis Type	Select the chassis type: Chassis 5050 or 5140.

IP Address	Enter the IP address of the Shelf Manager running on the chassis.
Chassis Slot Assignment	You cannot assign FortiGate-5000 series blades to the slot until after the chassis has been added. For information on assigning slots, see "To edit a chassis and assign FortiGate-5000 series blade to the slots" on page 114.

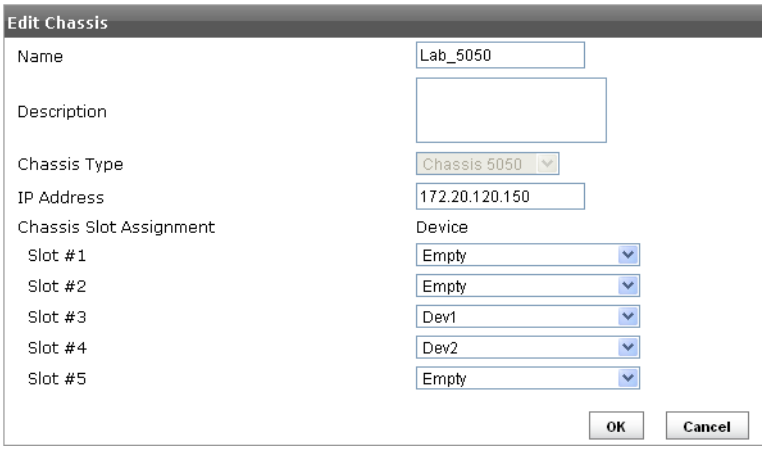
3 Select *OK*.

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

1 In the Navigation Pane, go to *Device Manager* > *Chassis*.

2 In the Content Pane, select the *Edit* icon of the chassis to edit.

Figure 68: Editing a chassis



3 Modify the fields except *Chassis Type* as required.

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.

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

5 Select *OK*.

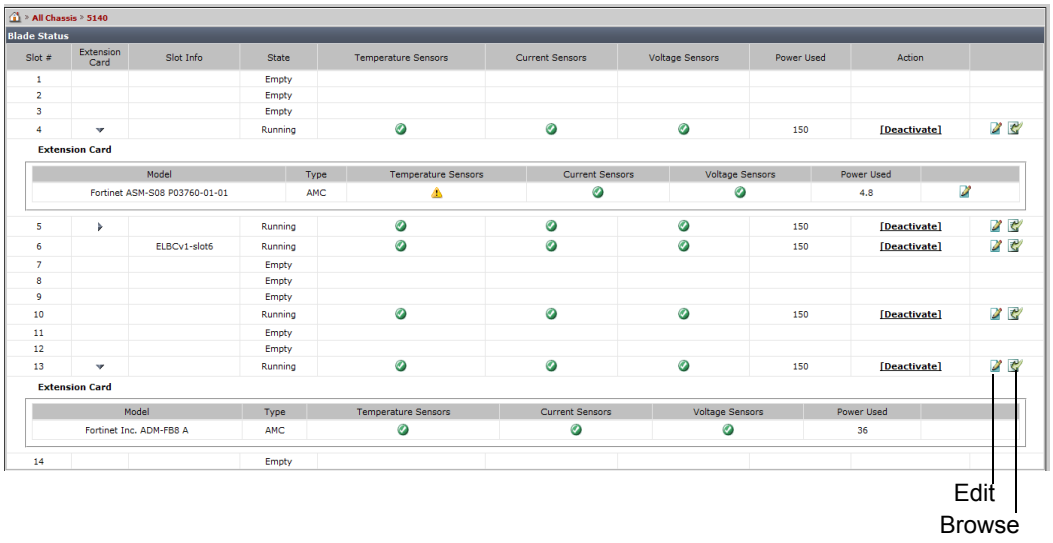
Viewing chassis dashboard

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 Nagivation Pane, go to *Device Manager* > *Chassis* and in the Content Pane, select the name of a chassis in the list. Optionally you can select Blade status from the Navigation pane when the Chassis has been selected.

Figure 69: Blade status



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 contains 5 slots numbered 1 to 5. The FortiGate-5140 contains 14 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 exanded 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.
Voltage Sensors	Indicates if the voltage sensors for the blade in each slot are detecting a voltage within an acceptable range.
Power Used	Indicates the amount of power being consumed by 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 icon	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. For more information, see “To edit voltage and temperature values” on page 116.
Browse icon	Select to update the slot.

To edit voltage and temperature values

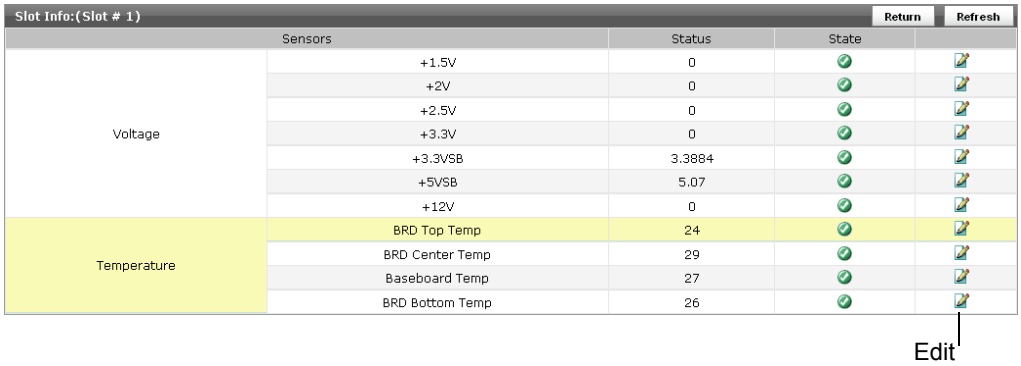
1 Go to *Device Manager* > *Chassis* and in the Content Pane select the name of a chassis in the list.

2 In the Navigation Pane, select the *Blades* item.

3 Select the *Edit* icon of a slot.

The detailed information on the voltage and temperature of the slot including sensors, status, and state displays.

Figure 70: Editing a slot



4 Select the *Edit* icon of a voltage or temperature sensor.

For a voltage sensor, you can modify the *Upper Non-critical, Upper Critical, Lower Non-critical*, and *Lower Critical* values.

For a temperature sensor, you can modify the *Upper Non-critical* and *Upper Critical* values.

5 Select *OK*.

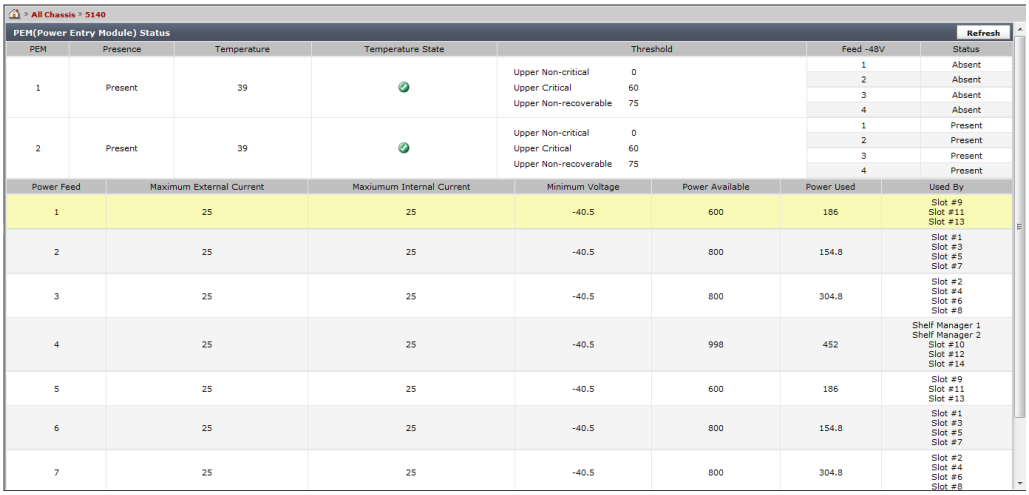
Viewing the status of the power entry modules

You can view the status of the power entry modules (PEM).

Go to *Device Manager* > *Chassis* and in the Content Pane select the name of a chassis in the list. In the Navigation Pane, select the *PEM* tab.

The FortiGate -5140 chassis displays more PEM information than the FortiGate -5050.

Figure 71: PEM status (FortiGate -5140 chassis)

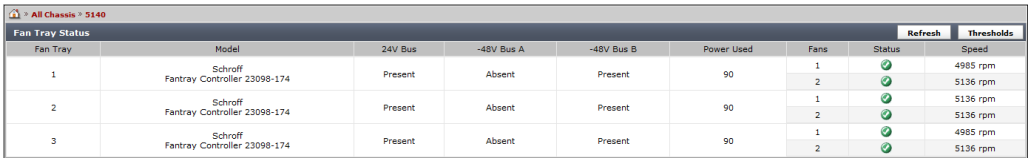


Refresh	Select to update the current page.
PEM	The order numbers of the PEM in the chassis.
Presence	Indicates whether the PEM is present or absent.
Temperature	The temperature of the PEM.
Temperature State	Indicates whether the temperature of the PEM is in the acceptable range. *OK* indicates that the 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 Used	Power used by each pair of fuses.
Used By	The slot that uses the power.

Viewing fan tray status (FortiGate-5140 chassis only)

Go to *Device Manager* > *Chassis* > *Chassis* and select the name of a FortiGate-5140 chassis in the list. Select the *Fan Tray* tab.

Figure 72: Fan tray status

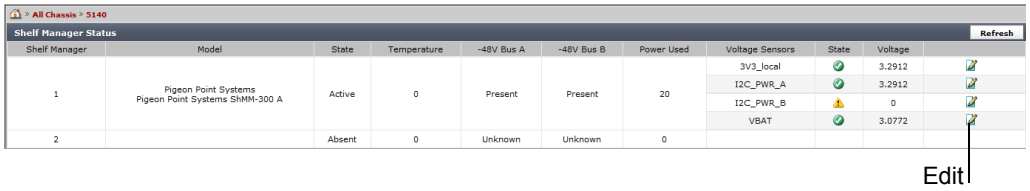


Refresh	Select to update the current page.
Thresholds	Displays the fan tray thresholds.
Fan Tray	The order numbers of the fan trays in the chassis.
Model	The fan tray model.
24V Bus	Status of the 24v Bus: present or absent.
-48V Bus A	**Status of the -48v Bus A: present or absent.**
-48V Bus B	**Status of the -48v Bus B: present or absent.**
Power Used	Power consumed by 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 *Device Manager* > *Chassis* and in the Content Pane select the name of a chassis in the list. In the Navigation Pane, select the *Shelf Manager* item.

Figure 73: Shelf Manager status



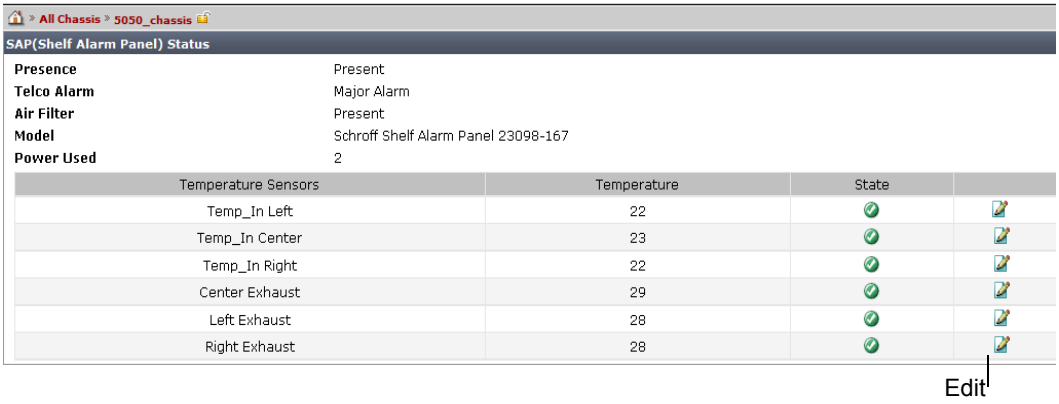
Refresh	Select to update the current page.
Shelf Manager	The order numbers of the shelf managers in the chassis.
Model	The shelf manager model.
State	The operation status of the shelf manager.
Temperature	The temperature of the shelf manager.
-48V Bus A	**Status of the -48v Bus A: present or absent.**
-48V Bus B	**Status of the -48v Bus B: present or absent.**
Power Used	Power consumed by 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.
Voltage	Voltage value for a voltage sensor.
Edit icon	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 *Device Manager* > *Chassis* and in the Content Pane select the name of a chassis in the list. In the Navigation Pane, select the *SAP* item.

Figure 74: SAP status



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 Used	Power consumed by 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 icon	Select to modify the thresholds of a temperature sensor.

Global Objects

The FortiManager system global database is called Global Objects. In the FortiManager system, an object is part of a device's configuration such as a firewall policy, a DNS server, a VPN console, an IP pool, or other such item. A global object is an object that is not associated specifically with one device or group. Objects that are associated with a device or group are part of the device database.

The Global Objects window is where you can configure global objects and copy the configurations to the FortiManager device database for a selected device or a group of devices. You can also import configurations from the FortiManager device database for a selected device and modify the configuration as required.

When configuring or creating a global policy object the interface, prompts, and fields are the same as creating the same object on a FortiGate unit using the FortiGate web-based manager. Therefore, this section does not provide the detailed steps for creating some complex global objects that you can find in the FortiGate unit documentation. This section only describes the differences that are not available on an individual device. Procedures on how to configure global objects

Note: When you copy a global object configuration to devices or groups, the configuration is sent to the FortiManager device database for the devices or groups. It is not installed on the actual devices or groups.
When you import a configuration, you copy it from the FortiManager device database for the selected device, not from the device itself.
For more information on the configuration workflow, see "Configuration and installation workflow" on page 18.

The following topics are included in this section:

Global objects window

The *Global Objects* window is similar to other components of the FortiManager system web-based user interface—a Navigation Pane is presented on the left side of the window and when you select objects in the Navigation Pane, object summary and configuration options are displayed in the Content Pane to the right.

To view the *Global Objects* window, from the Navigation Pane select *Global Objects*, and then select an object.

Differences between EMS and GMS modes

In EMS mode, the Global Objects window contains the Policy Objects and Device Settings lists. In GMS mode, the Global Objects window has the Device Settings objects. The Policy Objects are found under Security Console including some additional objects such as Virtual IP, Load Balancing, Control List, and Data Leak Prevention. See "Dynamic Objects" on page 206.

The added objects in GMS mode are often required in large company networks where the configurations must be controlled across the network to ensure corporate security policies are followed on all devices. In EMS mode where this cannot be enforced, these features are not present.

In GMS mode when configuring policy objects, there is an option to assign a color to that object. This helps group objects by use or device.

Screen captures in this chapter show EMS mode unless otherwise specified.

Figure 75: Global Objects window in EMS mode

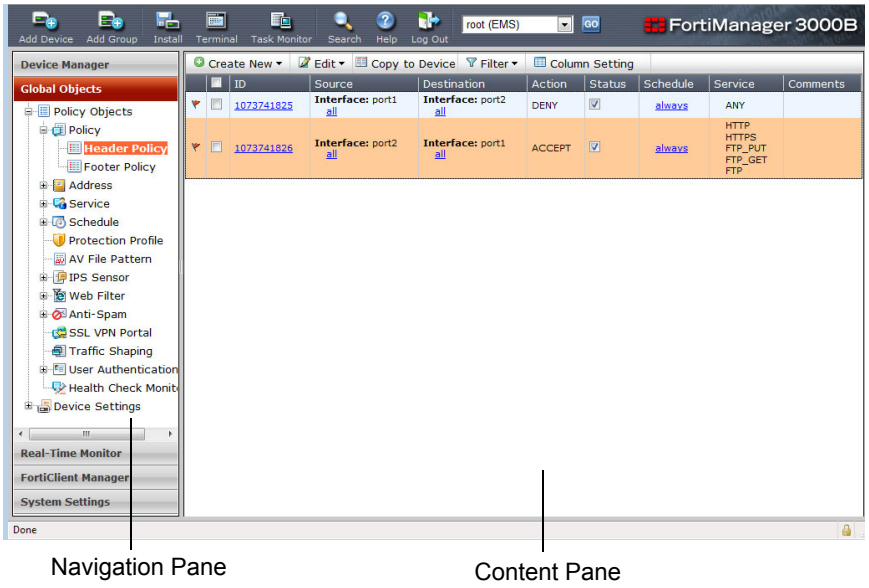


Figure 76: Global Objects window in GMS mode

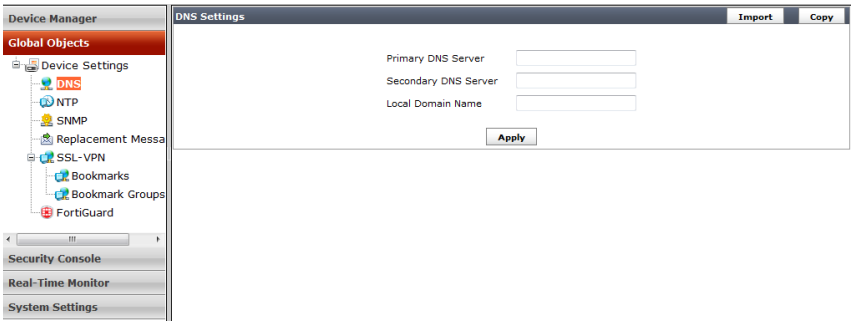
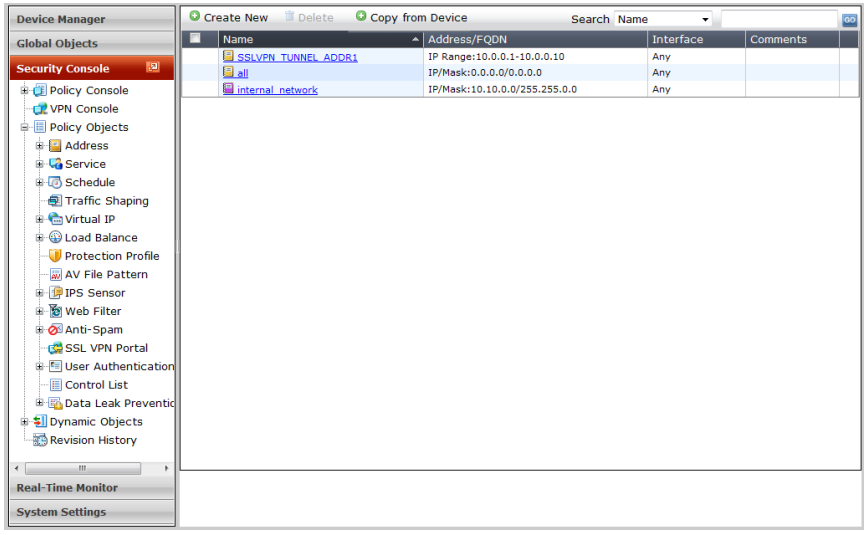


Figure 77: Policy Objects window in GMS mode



Global objects Navigation Pane

The Navigation Pane displays the list of global object categories. The Content Pane displays the summary and configuration options for the selected global object category. The objects in the Content Pane reflect information that is present in the FortiManager repository.

Some global objects only are available in GMS or EMS mode. Where applicable, this is indicated in the following table.

The Navigation Pane has the following items:

Policy Objects	In GMS mode, *Policy Objects* are found under *Security Console.* See “Security Console” on page 197.
Policy (EMS only)	In EMS mode, select to view and configure firewall policies in the categories of header and footer. By default there are no differences between the two categories. Administrators can use these categories for firewall policies that are typically are checked first (header) or last (footer) in the list. For more information, see “Configuring firewall policies” on page 129 In GMS mode under Security Console there is also a Policy item (see “Dynamic Objects” on page 206), but it is not for policy objects.
Address	Select to view and configure firewall addresses and address groups. For more information, see “Configuring firewall addresses” on page 132 and “Configuring firewall address groups” on page 133.
Service	Select to view and configure predefined firewall services, firewall services, and service groups. For more information, see “Viewing predefined firewall service list” on page 133, “Configuring custom services” on page 134 and “Configuring firewall service groups” on page 134.
Schedule	Select to view and configure recurring and one-time schedules. For more information, see “Configuring firewall schedules” on page 135.
Traffic Shaping	Select to view and configure traffic shapings that control the bandwidth available to, and set the priority of the traffic processed by, the firewall policy. Traffic shaping makes it possible to control which policies have the highest priority when large amounts of data are moving through the device. For more information, see “Configuring traffic shaping (EMS mode)” on page 159.

Virtual IP (GMS only)	In GMS mode, select to view and configure VIPs and VIP groups. For more information, see “Configuring virtual IPs” on page 183 and “Configuring virtual IP groups” on page 185.
Load Balance (GMS only)	In GMS mode, select to view and configure virtual servers, real servers, or configure a device’s health check monitors. For more information, see “Configuring load balancing” on page 169.
Protection Profile	Select to view and configure firewall protection profiles. For more information, see “Configuring firewall protection profile” on page 136.
AV File Pattern	Select to display and configure antivirus file patterns. For more information, see “Configuring global antivirus file pattern” on page 137.
IPS Sensor	Select to view and configure IPS sensors. This item includes IPS Sensor, IPS DoS Sensor, and IPS Custom Signature. For more information, see “Configuring IPS sensors” on page 138, “Configuring pre-defined and custom overrides” on page 141, “Configuring IPS DoS sensors” on page 143, and “Configuring IPS custom signatures” on page 144.
Web Filter	Select to view and configure the filter lists for Web content filtering, URL blocking, and local categories. For more information, see “Configuring global web filters” on page 146.
Anti-Spam	Select to view and configure the spam filters including IP addresses, email addresses, and banned words. For more information, see “Configuring global spam filters” on page 153.
SSL VPN Portal	Select to view and import SSL VPN portals from a device. For more information, see “Configuring SSL VPN portal” on page 159.
User Authentication	Select to view and configure user accounts, user groups, and external authentication servers including RADIUS, LDAP, TACAS+, and PKI servers. For more information, see “Configuring user authentication” on page 160.
Control List (GMS only)	In GMS mode, select to view and configure application control list. For more information, see “Configuring application control list” on page 174.
Health Check Monitor (EMS only)	In EMS mode, select to view and configure health check monitors. A health check occurs every number of seconds indicated by the interval. If a reply is not received within the timeout period, and you have configured the health check to retry, it will attempt a health check again; otherwise, the virtual server is deemed unresponsive, and load balancing will compensate by disabling traffic to that server until it becomes responsive again. For more information, see “Configuring health check monitors” on page 172. In GMS mode, health check monitor is part of Load Balancing.
Data Leak Prevention	Select to view and configure data leak prevention including sensors, compounds, and rules. For more information, see “Configuring data leak prevention” on page 177.
Device Settings	
DNS	Select to view and create DNS servers and domain. For more information, see “Configuring DNS” on page 186.
NTP	Select to view and configure a network time protocol (NTP) server. For more information, see “Configuring NTP” on page 187.
SNMP	Select to configure the SNMP agent settings for managed devices to report their system information and send traps (alarms or event messages) to SNMP managers. For more information, see “Configuring SNMP” on page 187.
Replacement Messages	Select to change replacement messages and customize alert information a FortiGate unit adds to content streams such as email messages, authentication pages, web pages, and FTP sessions. For more information, see “Configuring replacement messages” on page 190.

SSL-VPN	Select to create hyperlink bookmarks or groups of bookmarks to frequently accessed server applications that the user can select to start any session from his or her home page. For more information, see “Configuring SSL VPN bookmarks” on page 191 and “Configuring SSL VPN bookmark groups” on page 194.
FortiGuard	Select to view and configure FortiGuard override settings for AV/IPS service or web filtering and AntiSpam. For more information, see “Configuring FortiGuard settings” on page 195.

Common configuration actions

In the *Global Objects* window, there are two locations for controls to help with common configuration actions — a list of common configuration actions accessible through the right-click menu, and the menu bar at the top of the Content Pane.

When configuring global objects in the Content Pane, if information appears to be missing expand your window as there may be additional information that will be displayed in a larger window.

Content Pane menu bar

The menu bar at the top of the Content Pane includes configuration actions such as Create New, Edit, Delete, Copy from Device, and Search. The available actions varies between objects and for more information on these actions, see the appropriate global object sections.

The Import button has the same functionality for all global objects.

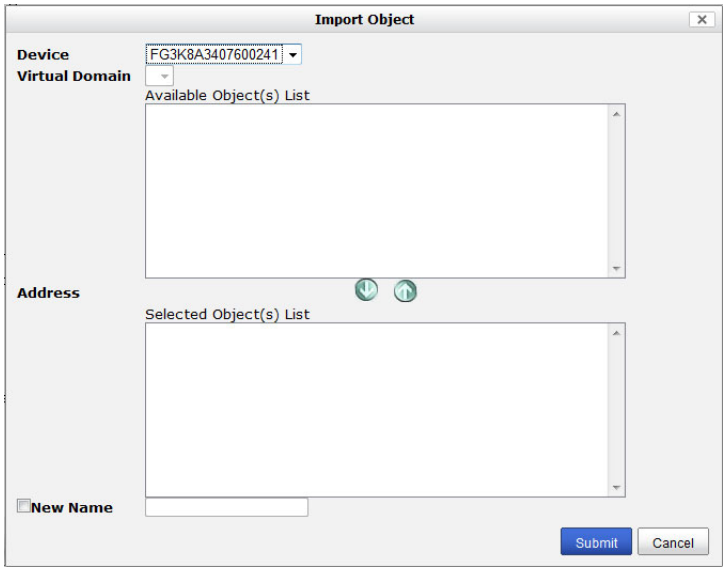
Copy a global object from a device

If you need to configure a global object that is very similar to an object that already exists on another device, you can import objects from that device to the global object database on the FortiManager system using the Import button on the Content Pane menu bar.

To import a global object

1. Select a global object category in the Navigation Pane.
2. In the Content Pane, select *Import*.

Figure 78: Importing global objects



3 Complete the following information:

Device	Select the device from which you want to import a global object.
Virtual Domain	If the device has Virtual domains, select the one from which you want to import a global object.
Available Object(s) List	Select the global object that you want to import from the *Available Object(s) List* field and move it to the *Selected Object(s) List* field using the right-pointing arrow. The objects in the Available Object(s) List are listed with their name followed by the device name, and virtual domain name if applicable. For example a firewall address called `Sales_network` on a device called `Sales_firewall` in a virtual domain called `vdom3` would appear in the list as `Sales Network (Sales_firewall[vdom3])`
New Name	If you want to rename the global object, select the checkbox and enter the new name for the object. Until you select the checkbox, you cannot enter a new name.

4 Select *OK*.

The imported global object appears on the global object list.

Right-click menu

There are common configuration actions for many global objects including delete, edit, clone, copy, clean up, query device database(s), search, and select all. These actions are accessed by right-clicking an object from the object list in the Content Pane. This will display a menu offering these actions.

Note: The menu displayed has different options than the menu for the policy objects policy list. See "Policy Right-click Options" on page 131.

Table 10: Right-click menu actions

Delete	Select to remove the highlighted object. Delete is not be available if the object cannot be deleted.
Edit	Select to change the configuration of the selected object. This is the same action as selecting the object name from the object list in the Content Pane. Edit is not available if multiple objects are selected.
Clone	Select as a quick way to create anew object similar to an existing global object.
Copy	Select to copy the global object to a device or device group saved in the FortiManager system device database.
Clean Up	Select to remove the global object from all devices where it is not used.
Query device database(s)	Select to discover if a global object has been copied to a device or device group that is saved in the FortiManager device database.
Search	Select to automatically search for occurrences of the selected object including which devices or databases it is part of, and what other objects refer to it if any.
Select All	Select to select all the objects in the list. This is in preparation for another action.

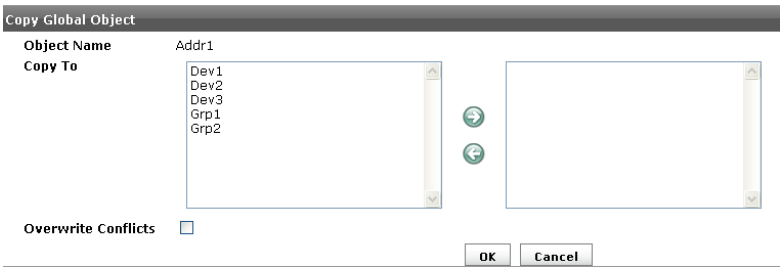
To copy a global object

1 Go to *Device Manager* and ensure the devices you want to copy the object to are locked. See "Device configuration locks" on page 69.

2 Select a global object category in the Navigation Pane.

3 In the Content Pane, select the *Copy* icon for the global object to be copied into the FortiManager device database.

Figure 79: Copying global objects



4 Complete the following information:

Object Name	The read-only name of the selected global object.
Copy To	Select the devices or groups in the list to which you want to copy the global object. Use the arrows to move the selected devices or groups between the lists. If device locking is enabled, no devices/groups appear in the list. For more information, see "Device configuration locks" on page 69.
Overwrite Conflicts	Select this checkbox to replace the existing global object with the same name on the FortiManager device databases for these devices or groups with the new global object. If you do not select this and there is a conflict on that device, the copy will not happen for that device.

5 Select *OK*.

The *Installation Progress* page appears, showing the copying status.

To query device database(s) for a global object

1 Select a global object category in the Navigation Pane.

2 In the Content Pane, select a global object from the list by right-clicking on it.

3 Select *Query Device Database(s)*.

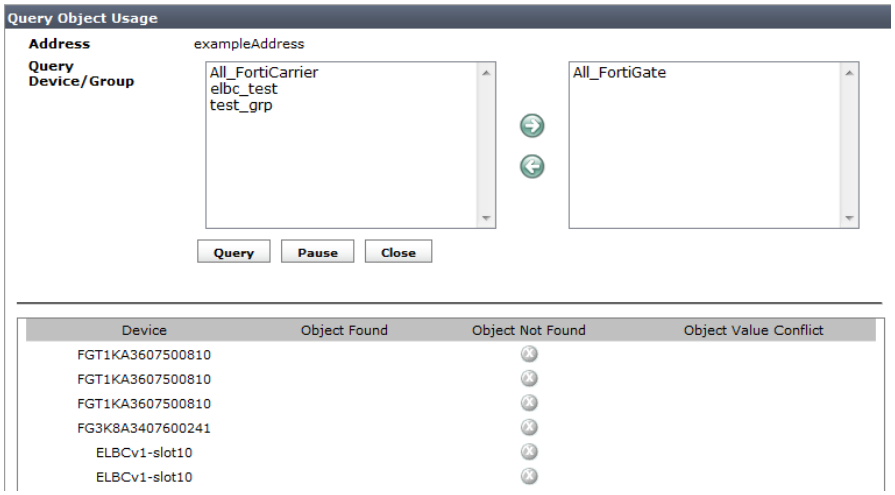
4 Select the device or devices to query from the left hand list and move them to the right hand list using the left and right arrows.

5 Select Query to start the search.

6 The results are displayed in the bottom window of the Content Pane. Information displayed includes device name, if the object was found or not, and if there was a conflict with the object.

7 To return to the object list, select the global object category.

Figure 80: Device database query for object usage



Configuring global policy objects

Configure global policy objects and copy the configurations to a selected FortiGate unit or device group saved in the FortiManager device database as required.

In GMS mode, the *Policy Objects* item is under *Security Console* in the Navigation Pane and there are additional object categories listed as indicated in "Security Console window" on page 197.

Among the tasks of configuring a global policy object, creating a global object using the *Device Manager* window is very similar to creating the same object on a FortiGate unit using the FortiGate web-based manager. Therefore, this section does not provide the detailed steps for creating some complex global objects that you can find in the FortiGate unit documentation. This section only describes the differences that are not available on an individual device.

It is assumed that you have one or more FortiGate units, and are familiar with configuring them before using the FortiManager system. For more information, see the FortiGate unit documentation for complete information on creating a global object. Complete FortiGate documentation is available from the FortiManager system CD. The most up-to-date FortiGate documentation is also available from Fortinet Technical Support.

Advanced policy objects

Most global policy objects are configured in the FortiManager system web-based interface as they are in the FortiGate unit web-manager interface. However, some policy objects involve two steps to configure, such as AV File Patterns. The first step configures the pattern entry, and the second step configures rules under it.

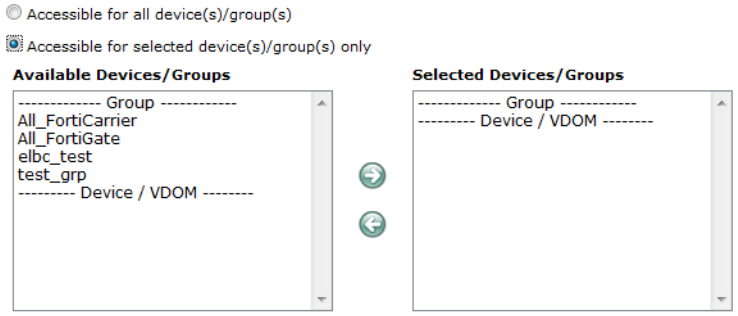
The advanced policy objects include the UTM objects — AV File Pattern, IPS Sensor, Web Filter, and Anti-Spam. While the procedure for configuring these objects is very similar to the process when using the FortiGate unit web-based manager interface, the two stage approach may be confusing.

Accessibility options - EMS mode

In EMS mode, each global object that you configure includes accessibility options at the bottom of the window. These options indicate if the global object is to be available to all devices or only to small set of devices or groups.

When you select the option *Accessible for selected device(s)/group(s) only*, the available and selected devices/groups lists appear and you can transfer groups and devices from one list to the other.

Figure 81: Accessibility options



Configuring firewall policies

In EMS mode, selecting the Policy item under Global Objects allows you to view or create firewall policies in one of two categories — header or footer.

By default there are no differences between header policies and footer policies. Header policies are intended to be at or near the top of the firewall policy list, and checked first for a match. Footer policies are intended for firewall policies that are located at or near the bottom of the policy list and will be checked for a match last. These two categories help administrators organize their firewall policies.

For easier reordering and copying of policies, you can click on a policy in the list and while holding the mouse button down move that policy to a new place in the list. When you let go of the mouse button, the policy list will reorder with the policy you moved being inserted in the new location.

Policy list - EMS mode

There are two options under Policy - Header and Footer. The display in the Content Pane for each is the same. The only difference that is visible is when you select Policy Copy it states if it is the Header database or the Footer database that is being pushed down to the device database. Otherwise, all controls apply to both Header and Footer policies.

For advanced policy manipulation, see "Policy Right-click Options" on page 131.

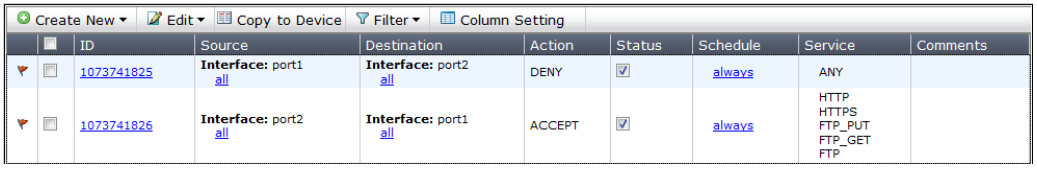
To add a Header firewall policy - EMS mode

1 In the Navigation Pane, go to *Global Objects* > *Policy Objects* > *Policy* > *Header Policy*.
2 In the Content Pane, select *Create New* and enter the firewall policy information.
3 Select the Accessibility options. See "Accessibility options - EMS mode" on page 129.
4 Select *OK* to confirm your policy configuration.

To add a Footer firewall policy - EMS mode

1 In the Navigation Pane, go to *Global Objects* > *Policy Objects* > *Policy* > *Footer Policy*.
2 In the Content Pane, select *Create New* and enter the firewall policy information.
3 Select the Accessibility options. See "Accessibility options - EMS mode" on page 129.
4 Select *OK* to confirm your policy configuration.

Figure 82: Policy list



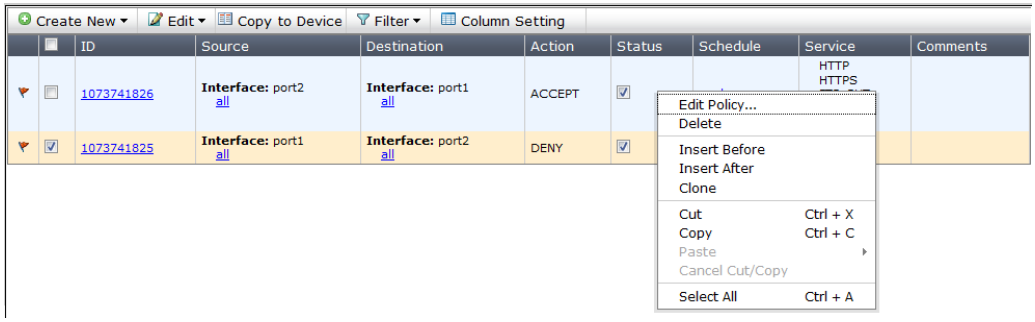
Create New	Select *Create New* to create a new policy or alternately select to create a section title. A section title groups a number of policies under a heading for easier reference.
Edit	Select *Edit* to Edit, Delete, or Move a policy. If multiple policies are selected, Delete is the only available option.
Copy to Device	Select to push the Header or Footer Policy database to each device database. A progress window is displayed.
Filter	Select to set or clear the filter. You can set a filter on any of the policy fields to limit the displayed policies. This can be useful for finding specific policies in a long list. Filters remain in place until *Clear* is selected.
Column Setting	Select to change which fields of the policies are displayed and in what order. Use the left and right arrows to display a field or remove it from being displayed. Use the up and down arrows to change a displayed field's position in the display. Up moves the field to the left.
Flag	A red flag indicates this change has not been saved. Install the policy to a device to remove this red flag. See "Installing Device Configurations" on page 277.

Seq. #	The sequence number indicates the order the policies will be checked. When policies are reordered, the sequence numbers remain in order.
ID	The unique ID number assigned to this policy.
Checkbox	Select one or more policies from the list using checkboxes. When selected right-click to bring up a menu of available actions. See "Policy Right-click Options" on page 131.
Source	The source interface and addresses for this policy.
Status	A check indicates this policy is enabled. Select the checkbox to enable or disable the policy.

Policy Right-click Options

Positioning the pointer over a policy in the policy list and right-clicking brings up a menu of options for reordering policies. Alternately you can use the checkboxes to select multiple policies before bringing up the right-click menu. With multiple policies selected, not all actions are available as some actions such as edit require a single policy.

Figure 83: Right-click policy list options



Edit Policy	Select to edit the selected policy.
Delete	Select to delete the selected policy. You can select multiple policies for deletion.
Insert Before	Create a new policy immediately before the selected policy.
Insert After	Create a new policy immediately after the selected policy.
Clone	Make an exact copy of the selected policy. The only difference will be the ID number. This is useful for quickly adding policies that are only different in one or two values. Selecting multiple policies to clone will result in all selected policies being cloned.
Cut **Copy** **Paste**	*Cut*, *Copy*, and *Paste* behavior is the same as for PC software applications. When you *Cut* a policy or policies until you *Paste* your selection, it remains greyed out in the policy list. *Paste* is not available if there is no policy or policies ready to paste.
Cancel Cut/Copy	Until you *Paste* your selection, the policy or policies that you *Cut* or Copied remain in the policy list. If you selected *Cut*, the selection remains greyed out until you *Paste* it to a new location. During the *Cut/Copy* and *Paste* operation, select *Cancel Cut/Copy* to undo the most recent *Cut* or *Copy* operation in progress.
Select All	Select to select all policies in the list. Alternately you can select multiple policies using checkboxes

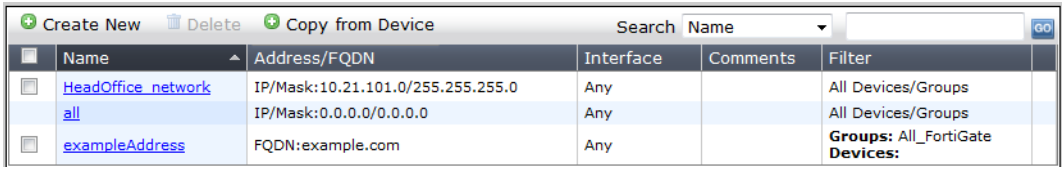
Configuring firewall addresses

To configure firewall addresses in EMS mode, go to *Global Objects* > *Policy Objects* > *Address* > *Address*. In GMS mode, go to *Security Console* > *Policy Objects* > *Address* > *Address*.

You can use one of two methods to represent hosts in firewall addresses: Subnet/IP Range or FQDN.

Caution: Be cautious if employing FQDN firewall addresses. Using a fully qualified domain name (FQDN) in a firewall policy, while convenient, does present some security risks. Policy matching then relies on a trusted DNS server. Should that DNS server be compromised, firewall policies requiring domain name resolution may no longer function properly.

Figure 84: Firewall address list



Create New	Select to add a firewall address.
Delete	Select the check box beside an address that you want to delete, then select *Delete* to remove the address. You cannot delete an address that is currently being used by a firewall policy or included in an address group.
Import	Select to import a firewall address from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the address list. Select *Name*, *Address/FQDN*, or *Comments* and enter the value to search, then select *GO*.
Checkbox	Select the checkbox of a address in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name of the firewall address. Select a name to view or edit the address.
Address/FQDN	The IP address or fully qualified domain name.
Comments	Any comments added for the firewall address.
Filter	EMS mode only. Display the devices and groups that can use the global firewall address configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

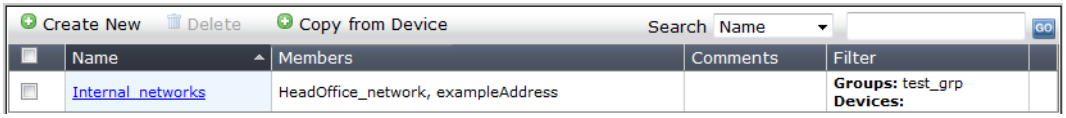
Configuring firewall address groups

You can organize multiple firewall addresses into an address group to simplify your firewall policy list. For example, instead of having five identical policies for five different but related firewall addresses, you might combine the five addresses into a single address group, which is used by a single firewall policy.

Because firewall policies require addresses with homogenous network interfaces, address groups should contain only addresses bound to the same network interface, or to Any — addresses whose selected Interface is Any are bound to a network interface during creation of a firewall policy, rather than during creation of the firewall address. For example, if address A1 is associated with port1, and address A2 is associated with port2, they cannot be grouped. However, if A1 and A2 have an Interface of Any, they can be grouped, even if the addresses involve different networks.

To configure firewall address groups in EMS mode, go to *Global Objects* > *Policy Objects* > *Address* > *Address Group*. In GMS mode, go to *Security Console* > *Policy Objects* > *Address* > *Address Group*.

Figure 85: Firewall address group list



Create New	Select to add an address group.
Delete	Select the check box beside an address group that you want to delete, then select *Delete* to remove the group. You cannot delete a group that is currently being used by a firewall policy or included in another address group.
Copy from Device	Select to import a firewall address group from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the address group list. Select *Name*, *Members*, or *Comments* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a group in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name of the firewall address group. Select a name to view or edit the address group.
Members	The addresses in the address group.
Comments	Any comments added for the firewall address group.
Filter	EMS mode only. Display the devices and groups that can use the global firewall address group configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

Viewing predefined firewall service list

Many well-known traffic types have been predefined in firewall services. These predefined services are defaults, and cannot be edited or removed. If you require service definitions that are different from the predefined services, you can add them using custom services. For more information, see "Configuring custom services" on page 134.

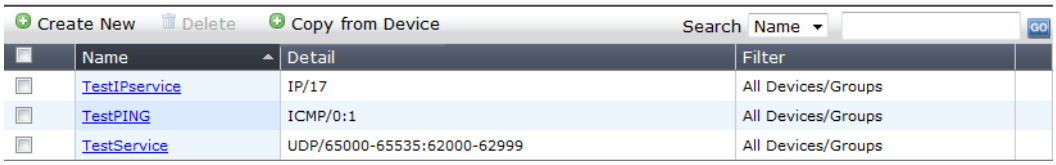
For more information on predefined firewall services, see the *FortiOS Administration Guide*.

Configuring custom services

Firewall services define one or more protocols and port numbers associated with each service. Service definitions are used by firewall policies to match session types. By default, the list of custom services is ordered alphabetically by service name.

To configure custom firewall services in EMS mode, go to *Global Objects* > *Policy Objects* > *Service* > *Custom*. In GMS mode, go to *Security Console* > *Policy Objects* > *Service* > *Custom*.

Figure 86: Firewall service list



Create New	Select to add a firewall service.
Delete	Select the check box beside a firewall service that you want to delete, then select *Delete* to remove the service. You cannot delete a service that is currently being used by a firewall policy or included in a service group.
Copy from Device	Select to import a firewall service from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the firewall service list. Select *Service Name* or *Detail* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a service in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name of the firewall service. Select a name to view or edit the firewall service.
Detail	The protocol and port numbers for each service. The information varies depending on the type of protocol selected.
Filter	EMS mode only. Display the devices and groups that can use the global firewall service configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

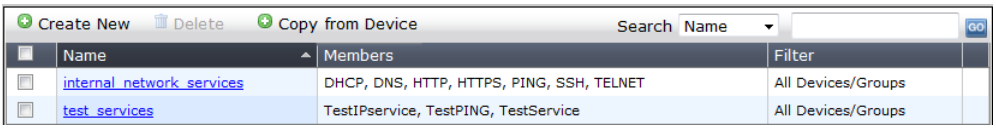
Configuring firewall service groups

You can organize multiple firewall services into a service group to simplify your firewall policy list. For example, instead of having five identical policies for five different but related firewall services, you might combine the five services into a single service group, which is used by a single firewall policy.

Service groups can contain both predefined and custom services.

To configure firewall service groups in EMS mode, go to *Global Objects* > *Policy Objects* > *Service* > *Service Group*. In GMS mode, go to *Security Console* > *Policy Objects* > *Service* > *Service Group*.

Figure 87: Firewall service group list



Create New	Select to add a service group.
Delete	Select the check box beside a firewall service group that you want to delete, then select *Delete* to remove the group. You cannot delete a group that is currently being used by a firewall policy or included in another service group.
Copy from Device	Select to import a firewall service group from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the firewall service group list. Select *Group Name* or *Members* and enter the value to search, then select *GO*.
Checkbox	Select the checkbox of a group in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name of the firewall service group. Select a name to view or edit the firewall service group.
Members	The members in the service group.
Filter	EMS mode only. Display the devices and groups that can use the global firewall service group configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

Configuring firewall schedules

You can create a recurring schedule that activates a policy during a specified period of time on an ongoing basis, or you can configure a one-time schedule that will only be in operation for one period of time. For example, you might prevent game play during office hours by creating a recurring schedule. Or if special work needs to be done around daylight savings time switch over, a one-time schedule could allow that and expire afterwards.

To configure firewall schedules in EMS mode, go to *Global Objects* > *Policy Objects* > *Schedule* and select either Recurring or One-time. In GMS mode, go to *Security Console* > *Policy Objects* > *Schedule* and do the same.

Note: A recurring schedule with a stop time that occurs before the start time starts at the start time and finishes at the stop time on the next day. You can use this technique to create recurring schedules that run from one day to the next. To create a recurring schedule that runs for 24 hours, set the start and stop times to the same time.

Figure 88: Firewall recurring schedule list

Figure 89: Firewall one-time schedule list

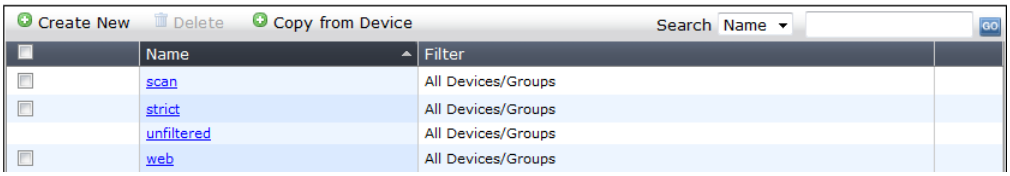
Create New	Select to add a firewall recurring schedule. For more information, see "Configuring firewall protection profile" on page 136.
Delete	Select the check box beside a schedule that you want to delete, then select *Delete* to remove the schedule. You cannot delete a schedule that is currently being used by a firewall policy.
Copy from Device	Select to import a firewall recurring schedule from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the firewall recurring schedule list. Select *Name, Day, Start,* or *Stop* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a schedule in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name of the firewall recurring schedule. Select a name to view or edit the schedule.
Day	The initials of the days of the week on which the schedule is active.
Start	The start time of the recurring schedule.
Stop	The stop time of the recurring schedule.
Filter	EMS mode only. Display the devices and groups that can use the global firewall recurring schedule configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

Configuring firewall protection profile

Protection profiles contain settings for many application layer and other types of protection, such as antivirus, web filtering, and logging, that you can apply to a firewall policy. Protection profiles can also contain settings for protocol-specific firewall actions, such as rate limiting for voice over IP (VoIP).

To configure firewall protection profiles in EMS mode, go to *Global Objects* > *Policy Objects* > *Protection Profile*. In GMS mode, go to *Security Console* > *Policy Objects* > *Protection Profile*.

Figure 90: Protection profile list



Create New	Add a protection profile. For more information, see "Configuring global antivirus file pattern" on page 137.
Delete	Select the check box beside a profile that you want to delete, then select *Delete* to remove the profile. You cannot delete a profile that is currently being used by a firewall policy.
Copy from Device	Select to import a firewall protection profile from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the firewall protection profile list. Select *Name* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a profile in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name of the protection profile. Select a name to view or edit the profile.
Filter	EMS mode only. Display the devices and groups that can use the global firewall protection profile configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

Configuring global antivirus file pattern

You can configure the antivirus file patterns to block files by file name, or file type. File pattern blocking provides the flexibility to block potentially harmful content.

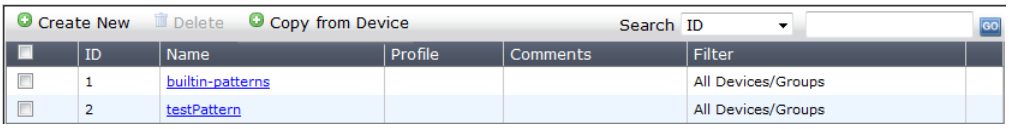
File pattern entries are not case sensitive. For example, adding `*.exe` to the file pattern list also blocks any files ending in `.EXE`.

Files can also be blocked by type, without relying on the file name to indicate what type of files they are. When blocking by file type, the FortiGate unit analyzes the file and determines the file type regardless of the file name.

To configure global antivirus file patterns in EMS mode, go to *Global Objects* > *Policy Objects* > *AV File Pattern* > *AV File Pattern*. In GMS mode, go to *Security Console* > *Policy Objects* > *AV File Pattern* > *AV File Pattern*.

For more information about antivirus file pattern, see the FortiGate documentation.

Figure 91: File pattern list



Create New	Select to add a new file pattern to the list. For more information, see "To add an AV file pattern and file pattern filter" on page 138.
Delete	Select the check box beside a file pattern that you want to delete, then select *Delete* to remove it. You cannot delete a file pattern if it is selected in a protection profile.
Copy from Device	Select to import a file pattern from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the file pattern list. Select *ID*, *Name,* or *Comment* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a pattern in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
ID	A unique identifier for each file pattern.
Name	The available file patterns. Select to view or edit a file pattern.
Profile	The protection profile each file pattern has been applied to.
Comment	Optional description of each file pattern.
Filter	Only displayed in EMS mode. Display the devices and groups that can use the antivirus file pattern configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add an AV file pattern and file pattern filter

1. Go to AV File Pattern. In EMS mode go to *Global Objects* > *Policy Objects* > *AV File Pattern* > *AV File Pattern*. In GMS mode, go to *Security Console* > *Policy Objects* > *AV File Pattern* > *AV File Pattern*.
2. Select *Create New*.
3. Enter the name of the new file pattern.
4. Enter a comment to describe the file pattern, if required.
5. Select *Apply*.

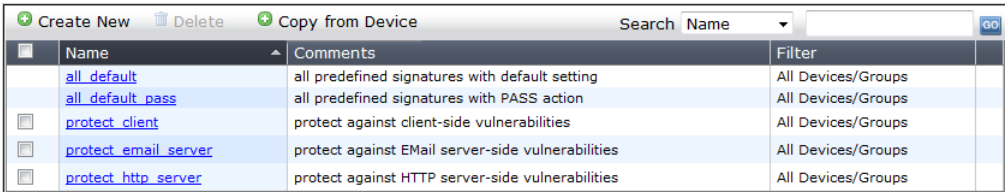
   The new file pattern is now added to the file pattern list.
6. Select *Create New.*
7. Select a Filter type of File name pattern or File type.
8. Enter the pattern or file type.
9. Select an *Action* of Block or Allow for each.
10. Select to Enable this file pattern.
11. Select *OK*.
12. Repeat steps 2 through 11 to add additional file patterns to this AV file pattern.
13. Select *Return* when done to return to the AV File Pattern list.

Configuring IPS sensors

You can group signatures into IPS (Intrusion Protection system) sensors for easy selection in protection profiles. You can define signatures for specific types of traffic in separate IPS sensors, and then select those sensors in profiles designed to handle that type of traffic.

The FortiGuard Service periodically updates the pre-defined signatures, with signatures added to counter new threats. Because the signatures included in filters are defined by specifying signature attributes, new signatures matching existing filter specifications will automatically be included in those filters. For example, if you have a filter that includes all signatures for the Windows operating system, your filter will automatically incorporate new Windows signatures as they are added.

Figure 92: IPS sensor list



Create New	Add a new IPS sensor. For more information, see "To add an IPS sensor" on page 139.
Delete	Select the check box beside an IPS sensor that you want to delete, then select *Delete* to remove the sensor.
Copy from Device	Select to import an IPS sensor from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the IPS sensor list. Select *Name* or *Comments* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a sensor in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name of each IPS sensor. Select a name to view or edit the sensor.
Comments	An optional description of the IPS sensor.
Filter	EMS mode only. Display the devices and groups that can use the global IPS sensor configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add an IPS sensor

1. Go to IPS sensor. In EMS mode, go to *Global Objects* > *Policy Objects* > *IPS Sensor* > *IPS Sensor*. In GMS mode, go to *Security Console* > *Policy Objects* > *IPS Sensor* > *IPS Sensor*.
2. In the Content Pane, select *Create New*.
3. Enter the name of the new sensor.
4. Enter a comment to describe the sensor, if required.
5. Select *Apply*.

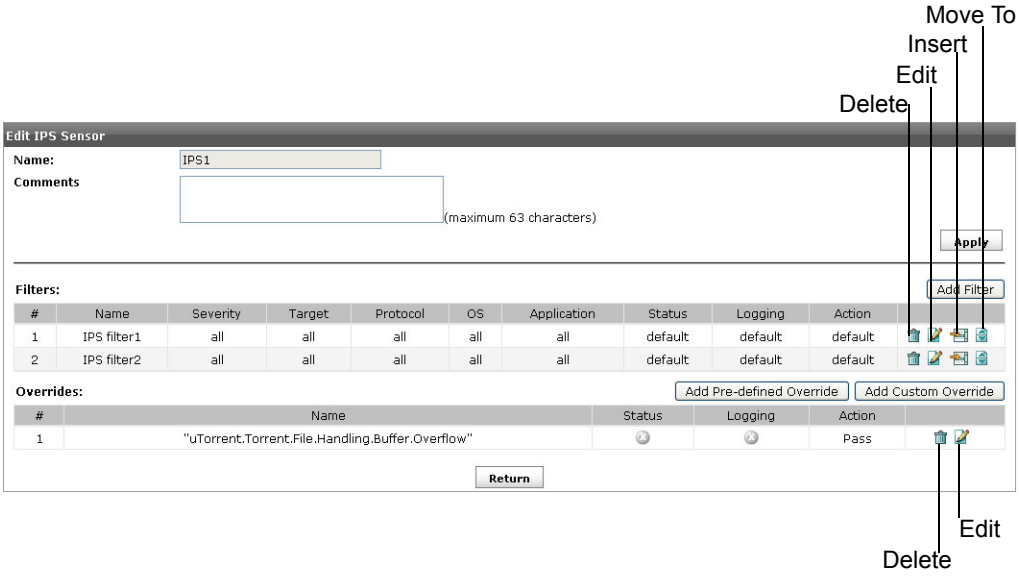
   The new IPS sensor appears on the list.
6. Select *Create New* to add Filters and Overrides. See "Configuring IPS custom signatures" on page 144.
7. Select *Return* to return to the IPS Sensor list.

To view the IPS sensor

1 Go to IPS Sensor. In EMS mode, go to *Global Objects* > *Policy Objects* > *IPS Sensor* > *IPS Sensor*. In GMS mode, go to *Security Console* > *Policy Objects* > *IPS Sensor* > *IPS Sensor*.

2 Select the name of the sensor to view.

Figure 93: IPS sensor



To add an IPS sensor filter

1 Go to IPS Sensor. In EMS mode, go to *Global Objects* > *Policy Objects* > *IPS Sensor* > *IPS Sensor*. In GMS mode, go to *Security Console* > *Policy Objects* > *IPS Sensor* > *IPS Sensor*.

2 Select the name of the IPS sensor containing the filter you want to edit.

3 Under Filters, select Create New.

4 Complete the following information:

Name	Enter or change the name of the IPS filter.
Severity	Select *All*, or select *Specify* and then one or more severity ratings. Severity defines the relative importance of each signature. Signatures rated critical detect the most dangerous attacks while those rated as info pose a much smaller threat.
Target	Select *All*, or select *Specify* and then the type of systems targeted by the attack. The choices are server or client.
OS	Select *All*, or select *Specify* and then select one or more operating systems that are vulnerable to the attack. Signatures with an OS attribute of All affect all operating systems. These signatures will be automatically included in any filter regardless of whether a single, multiple, or all operating systems are specified.
Protocol	Select *All*, or select *Specify* to list what network protocols are used by the attack. Use the Right Arrow to move the ones you want to include in the filter from the Available to the Selected list, or the Left Arrow to remove previously selected protocols from the filter.
Application	Select *All*, or select *Specify* to list the applications or application suites vulnerable to the attack. Use the Right Arrow to move the ones you want to include in the filter from the Available to the Selected list, or the Left Arrow to remove previously selected protocols from the filter.
Configuration	
Enable	Select from the options to specify what the device will do with the signatures included in the filter: enable all, disable all, or enable or disable each according to the individual default values shown in the signature list.
Logging	Select from the options to specify whether the device will create log entries for the signatures included in the filter: enable all, disable all, or enable or disable logging for each according to the individual default values shown in the signature list.
Action	Select from the options to specify what the device will do with traffic containing a signature match: pass all, block all, reset all, or block or pass traffic according to the individual default values shown in the signature list.

The signatures included in the filter are only those matching all attributes specified. When created, a new filter has every attribute set to *all* which causes every signature to be included in the filter. If the severity is changed to high, and the target is changed to server, the filter includes only signatures checking for high priority attacks targeted at servers.

5 Select *OK*.

Configuring pre-defined and custom overrides

Pre-defined and custom overrides are configured and work mainly in the same way as filters. Unlike filters, each override defines the behavior of one signature.

Overrides can be used in two ways:

- To change the behavior of a signature already included in a filter. For example, to protect a web server, you could create a filter that includes and enables all signatures related to servers. If you wanted to disable one of those signatures, the simplest way would be to create an override and mark the signature as disabled.
- To add an individual signature, not included in any filters, to an IPS sensor. This is the only way to add custom signatures to IPS sensors.

When a pre-defined signature is specified in an override, the default status and action attributes have no effect. These settings must be explicitly set when creating the override.

Note: Before an override can affect network traffic, you must add it to a filter, and you must select the filter in a protection profile applied to a policy. An override does not have the ability to affect network traffic until these steps are taken.

To add a pre-defined or custom override

1 Go to IPS Sensor. In EMS mode, go to *Global Objects* > *Policy Objects* > *IPS Sensor* > *IPS Sensor*. In GMS mode, go to *Security Console* > *Policy Objects* > *IPS Sensor* > *IPS Sensor*.

2 Select the name of the IPS sensor containing the override you want to edit.

3 Select *Add Pre-defined Override* or *Add Custom Override*.

4 Complete the following:

Signature	Select the browse icon to view the list of available signatures. From this list, select a signature the override will apply to and then select *OK*.
Enable	Select to enable the signature override.
Action	Select *Pass* or *Block*. When the override is enabled, the action determines what the FortiGate will do with traffic containing the specified signature.
Logging	Select to enable creation of a log entry if the signature is discovered in network traffic.
Packet Log	Select to save packets that trigger the override to the FortiGate hard drive for later examination.
Quarantine Attackers (to Banned Users List)	Select to enable NAC quarantine for this override. For more information about NAC quarantine, see the *FortiGate Administration Guide*. The FortiGate unit deals with the attack according to the IPS sensor or DoS sensor configuration regardless of this setting.
Method	Select *Attacker's IP address* to block all traffic sent from the attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected. Select *Attacker and Victim IP Addresses* to block all traffic sent from the attacker's IP address to the target (victim's) IP address. Traffic from the attacker's IP address to addresses other than the victim's IP address is allowed. The attacker's and target's IP addresses are added to the banned user list as one entry. Select *Attack's Incoming Interface* to block all traffic from connecting to the FortiGate interface that received the attack. The interface is added to the banned user list.
Expires	You can select whether the attacker is banned indefinitely or for a specified number of days, hours, or minutes.
Exempt IP	Enter IP addresses to exclude from the override. The override will then apply to all IP addresses except those defined as exempt. The exempt IP addresses are defined in pairs, with a source and destination, and traffic moving from the source to the destination is exempt from the override.
Source	The exempt source IP address. Enter `0.0.0.0/0` to include all source IP addresses.
Destination	The exempt destination IP address. Enter `0.0.0.0/0` to include all destination IP addresses.
Add	Select to add the override.

5 Select *OK*.

Configuring IPS DoS sensors

The IPS uses a traffic anomaly detection feature to identify network traffic that does not fit known or common traffic patterns and behavior. For example, one type of flooding is the denial of service (DoS) attack that occurs when an attacking system starts an abnormally large number of sessions with a target system. The large number of sessions slows down or disables the target system so legitimate users can no longer use it. This type of attack gives the DoS sensor its name, although it is capable of detecting and protecting against a number of anomaly attacks.

You can enable or disable logging for each traffic anomaly, and configure the detection threshold and action to take when the detection threshold is exceeded.

You can create multiple DoS sensors. Each sensor consists of 12 anomaly types that you can configure. Each sensor examines the network traffic in sequence, from top to bottom. When a sensor detects an anomaly, it applies the configured action. Multiple sensors allow great granularity in detecting anomalies because each sensor can be configured to examine traffic from a specific address, to a specific address, on a specific port, in any combination.

When arranging the DoS sensors, place the most specific sensors at the top and the most general at the bottom. For example, a sensor with one protected address table entry that includes all source addresses, all destination addresses, and all ports will match all traffic. If this sensor is at the top of the list, no subsequent sensors will ever execute.

The traffic anomaly detection list can be updated only when the device firmware image is upgraded.

Figure 94: IPS DoS sensor list

Create New	Add a new DoS sensor.
Delete	Select the check box beside a DoS sensor that you want to delete, then select *Delete* to remove the sensor.
Copy from Device	Select to import a DoS sensor from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the DoS sensor list. Select *ID*, *Name* or *Comments* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a sensor in the list, and right-click to delete, edit, insert, move, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name of each DoS sensor. Select a name to view or edit the sensor.
Comments	An optional description of the DoS sensor.
Status	Select to enable this sensor.
Filter	EMS mode only. Display the devices and groups that can use the global DoS sensor configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration.

To add an IPS DoS sensor

1 Go to IPS DoS Sensor. In EMS mode, go to *Global Objects* > *Policy Objects* > *IPS Sensor* > *IPS DoS Sensor*. In GMS mode, go to *Security Console* > *Policy Objects* > *IPS Sensor* > *IPS DoS Sensor*.

2 Select *Create New*.

3 Enter the name of the new sensor.

4 Enter a comment to describe the sensor, if required.

5 Select *Apply*.

The new IPS DoS sensor appears on the list.

To view or edit the IPS DoS sensor

1 Go to IPS DoS Sensor. In EMS mode, go to *Global Objects* > *Policy Objects* > *A IPS Sensor* > *IPS DoS Sensor*. In GMS mode, go to *Security Console* > *Policy Objects* > *IPS Sensor* > *IPS DoS Sensor*.

2 Select the name of the sensor you want to view or edit.

3 Complete the following:

Name	File DoS sensor name. This is read-only.
Comments	Optional comment.
Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global DoS sensor configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global DoS sensor configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.
Anomalies Configuration	
Name	The name of the anomaly.
Enable	Select the check box to enable the DoS sensor to detect when the specified anomaly occurs. Selecting the check box in the header row will enable sensing of all anomalies.
Logging	Select the check box to enable the DoS sensor to log when the anomaly occurs. Selecting the check box in the header row will enable logging for all anomalies. Anomalies that are not enabled are not logged.
Action	Select Pass to allow anomalous traffic to pass when the FortiGate unit detects it, or set Block to prevent the traffic from passing.
Threshold	Display the number of sessions/packets that must show the anomalous behavior before the device triggers the anomaly action (pass or block). If required, change the number.

4 Select *OK*.

Configuring IPS custom signatures

Custom signatures provide the power and flexibility to customize the device's Intrusion Protection system for diverse network environments. The device predefined signatures represent common attacks. If you use an unusual or specialized application or an uncommon platform, you can add custom signatures based on the security alerts released by the application and platform vendors.

You can also create custom signatures to help you block P2P protocols.

After creation, you need to specify custom signatures in IPS sensors created to scan traffic. For more information about creating IPS sensors, see “Configuring IPS sensors” on page 138.

For more information about custom signatures, see the *FortiGate Intrusion Protection System (IPS) Guide*.

Figure 95: IPS custom signature list

Create New	Add a new signature.
Delete	Select the check box beside a signature that you want to delete, then select *Delete* to remove the signature.
Copy from Device	Select to import a signature from the selected device in the FortiManager device database. For more information, see “To import a global object” on page 125.
Search	Search the signature list. Select *Name* or *Signature* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a signature in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see “Right-click menu” on page 126.
Name	The custom signature name. Select a name to view or edit the signature.
Signature	The signature syntax.
Filter	EMS mode only. Display the devices and groups that can use the IPS custom signature configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see “Accessibility options - EMS mode” on page 129.

To add an IPS custom signature

1. Go to IPS Custom Signature. In EMS mode, go to *Global Objects* > *IPS Sensor* > *IPS Custom Signature*. In GMS mode, go to *Security Console* > *Policy Objects* > *IPS Sensor* > *IPS Custom Signature*.
2. Select *Create New*.
3. Enter the name of the new signature.
4. Enter the custom signature, using the appropriate syntax. For more information, see “Custom signature syntax” in the *FortiGate UTM User Guide*.
5. Select *OK*.

   The new IPS custom signature appears on the list.

Note: Custom signatures are an advanced feature. This document assumes the user has previous experience creating intrusion detection signatures.

Note: Custom signatures must be added to a signature override in an IPS filter to have any effect. Creating a custom signature is a necessary step, but a custom signature does not affect traffic simply by being created.

Configuring global web filters

Web filters are used to block certain web pages and emails based on the settings you select.

FortiManager web filter lists include web content block list, web content exempt list, and URL filter list.

For more information about global web filters, see the FortiGate documentation.

Configuring web content block

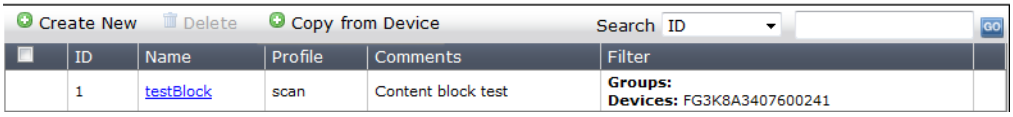
Control web content by blocking specific words or patterns. If enabled in the protection profile, the device searches for words or patterns on requested web pages. If matches are found, values assigned to the words are totalled. If a user-defined threshold value is exceeded, the web page is blocked.

Use Perl regular expressions or wildcards to add banned word patterns to the list.

Note: Perl regular expression patterns are case sensitive for Web Filter content block. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` blocks all instances of `bad language` regardless of case. Wildcard patterns are not case sensitive.

You can add multiple web content blocks and then select the best web content block for each protection profile.

Figure 96: Content block list



Create New	Select to add a new content block.
Delete	Select the check box beside a content block that you want to delete, then select *Delete* to remove it. You cannot delete a content block if it is included in a protection profile.
Copy from Device	Select to import a content block from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the content block list. Select *ID*, *Name,* or *Comment* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of an entry in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The available web content block lists. Select to view or edit the list.
Profile	The protection profile each web content block list has been applied to.
Comments	Optional description of each content block list.
Filter	EMS mode only. Display the devices and groups that can use the global content block configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add a content block

1 Go to Web Content Block. In EMS mode, go to *Global Objects* > *Policy Objects* > *Web Filter* > *Web Content Block*. In GMS mode, go to *Security Console* > *Policy Objects* > *Web Filter* > *Web Content Block*.

2 In the Content Pane, select *Create New*.

3 Enter the name of the new content block.

4 Enter a comment to describe the content block, if required.

5 Select *Apply*.

The new content block appears on the content block list.

To view or edit the content block

1 Go to Web Content Block. In EMS mode, go to *Global Objects* > *Policy Objects* > *Web Filter* > *Web Content Block*. In GMS mode, go to *Security Console* > *Policy Objects* > *Web Filter* > *Web Content Block*.

2 In the Content Pane, select the name of the content block you want to view or edit.

3 Complete the following:

Name	Content block name. This is read-only.
Comment	Optional comment. To add or edit comment, enter text and select *Apply*.
Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global content block configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global content block configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.
Apply	If you make changes to the content block, select to save the changes.
Create New	Select to add a new content block pattern to the file pattern list.
Pattern	The available content block patterns.
Pattern type	The pattern type used in the pattern list entry. Choose from wildcard or regular expression.
Language	The character set to which the content block belongs: *Western, Chinese Simplified, Chinese Traditional, Japanese, Korean, French, Thai, Spanish,* or *Cyrillic*.
Score	A numerical weighting applied to the pattern. The score values of all the matching patterns appearing on a page are added, and if the total is greater than the threshold value set in the protection profile, the page is blocked.
Status	Displays if the content block pattern is activated.
Return	Select to exit the content block page.

To add a content block filter

1 Go to Web Content Block. In EMS mode, go to *Global Objects* > *Policy Objects* > *Web Filter* > *Web Content Block*. In GMS mode, go to *Security Console* > *Policy Objects* > *Web Filter* > *Web Content Block*.

2 In the Content Pane, select the name of a content block.

3 Select *Create New*.

4 Complete the following:

Entry	The name of this filter. This is read only.
Pattern	Enter the content block pattern.
Pattern Type	Select a pattern type from the dropdown list: Wildcard or regular Expression.
Language	Select a character set to which the content block filter belongs: *Western, Chinese Simplified, Chinese Traditional, Japanese, Korean, French, Thai, Spanish,* or *Cyrillic*.
Score	Enter a score for the pattern.
Enable	Select to enable the pattern.

5 Select *Ok*.

Configuring web content exempts

Web content exempt allows overriding of the web content block feature. If any patterns defined in the web content exempt list appear on a web page, the page will not be blocked even if the web content block feature would otherwise block it.

You can add multiple web content exempts and then select the best web content exempt for each protection profile.

Figure 97: Web content exempt list

Create New	Select to add a new web content exempt. For more information, see "To add a web content exempt entry" on page 149.
Delete	Select the check box beside a content exempt that you want to delete, then select *Delete* to remove it. You cannot delete the content exempt if it is included in a protection profile.
Copy from Device	Select to import a web content exempt from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the content block list. Select *ID*, *Name,* or *Comment* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of an entry in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
ID	The identification number for the content exempt.
Name	The available web content exempts. Select a name to view or edit.
Profile	The protection profiles each web content exempt has been applied to.
Comments	Optional description of each web content exempt.
Filter	EMS mode only. Display the devices and groups that can use the global web content exempt configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add a web content exempt entry

1 Go to Web Content Exempt. In EMS mode, go to *Global Objects* > *Policy Objects* > *Web Filter* > *Web Content Exempt*. In GMS mode, go to *Security Console* > *Policy Objects* > *Web Filter* > *Web Content Exempt*.

2 In the Content Pane, select *Create New*.

3 Enter the name of the new content exempt entry.

4 Enter a comment to describe the content exempt, if required.

5 Select *Apply*.

The new content exempt entry appears on the web content exempt list.

To view or edit the web content exempt

1 Go to Web Content Exempt. In EMS mode, go to *Global Objects* > *Policy Objects* > *Web Filter* > *Web Content Exempt*. In GMS mode, go to *Security Console* > *Policy Objects* > *Web Filter* > *Web Content Exempt*.

2 In the Content Pane, select the name of the content exempt you want to view or edit.

3 Complete the following:

Name	Web content exempt name. This is read-only.
Comments	Optional comments. To add or edit comments, enter text and select *Apply*.
Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global web content exempt configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global web content exempt configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.
Create New	Select to add a new content exempt pattern to the file pattern list.
Checkbox	Select one or more entries in the file pattern list. When selected, right-click to display a menu of available actions - delete, edit, or select all. Edit will not be available if multiple entries are selected. See “Accessibility options - EMS mode” on page 129.
Pattern	The available web content exempt patterns. Select to edit the entry.
Pattern type	The pattern type used in the web content exempt filter. Choose from wildcard or regular expression.
Language	The character set to which the web content exempt filter belongs: *Western, Chinese Simplified, Chinese Traditional, Japanese, Korean, French, Thai, Spanish,* or *Cyrillic*.
Status	Display if the web content exempt filter is activated.
Delete icon	Select to remove the filter from the list.
Edit icon	Select to edit the filter.
Return	Select to exit the web content exempt page.

To add a web content exempt filter

1 Go to Web Content Exempt. In EMS mode, go to *Global Objects* > *Policy Objects* > *Web Filter* > *Web Content Exempt*. In GMS mode, go to *Security Console* > *Policy Objects* > *Web Filter* > *Web Content Exempt*.

2 In the Content Pane, select the name of a web content exempt.

3 Select *Create New*.

4 Complete the following:

Entry	The name of this filter. This is read only.
Pattern	Enter the web content exempt pattern.
Pattern Type	Select a pattern type from the dropdown list: Wildcard or regular Expression.
Language	Select one of the languages from the menu: *Western, Chinese Simplified, Chinese Traditional, Japanese, Korean, French, Thai, Spanish,* or *Cyrillic*.
Enable	Select to enable the filter.

5 Select *Ok*.

Configuring URL filters

Allow or block access to specific URLs by adding them to the URL filter list. Add patterns using text and regular expressions (or wildcard characters) to allow or block URLs.

Figure 98: URL filter list

Create New	Select to add a new URL filter. For more information, see "To add a URL filter" on page 150.
Delete	Select the check box beside a URL filter that you want to delete, then select *Delete* to remove it. You cannot delete the URL filter if it is included in a protection profile.
Copy from Device	Select to import a URL filter from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the URL filter list. Select *ID*, *Name,* or *Comment* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a filter in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
ID	The identification number for the URL filter.
Name	The available URL filters. Select to view or edit a list.
Profile	The protection profiles each URL filter has been applied to.
Comments	Optional description of each URL filter.
Filter	EMS mode only. Display the devices and groups that can use the global URL filter configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add a URL filter

1 Go to *Global Objects* > *Policy Objects* > *Web Filter* > *Web URL Filter*.

2 In the Content Pane, elect *Create New*.

3 Enter the name of the new URL filter.

4 Enter a comment to describe the URL filter, if required.

5 Select *Apply*.

The new URL filter appears on the URL filter list.

To view or edit the URL filter

1 Go to Web URL Filter. In EMS mode, go to *Global Objects* > *Policy Objects* > *Web Filter* > *Web URL Filter*. In GMS mode, go to *Security Console* > *Policy Objects* > *Web Filter* > *Web URL Filter*.

2 In the Content Pane, select the name of the URL filter you want to view or edit.

3 Complete the following:

Name	URL filter name. This is read-only.
Comments	Optional comment. To add or edit comment, enter text and select *Apply*.
Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global URL filter configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global URL filter configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.
Create New	Select to add a new URL filter pattern to the URL filter.
Checkbox	Select one or more entries in the URL filter list. When selected, right-click to display a menu of available actions - delete, edit, or select all. Edit will not be available if multiple entries are selected. See “Accessibility options - EMS mode” on page 129.
URL	The available URL filter entries.
Action	The action taken when the URL matches: *Allow*, *Block*, or *Exempt*. An allow match exits the URL filter list and checks the other web filters. An exempt match stops all further checking including AV scanning. A block match blocks the URL and no further checking will be done.
Type	The type of URL: Simple or Regex (regular expression).
Status	Display if the URL filter list entry is activated.
Edit icon	Select to edit the entry.
Return	Select to exit the URL filter page.

To add a URL filter pattern

1 Go to Web URL Filter. In EMS mode, go to *Global Objects* > *Policy Objects* > *Web Filter* > *Web URL Filter*. In GMS mode, go to *Security Console* > *Policy Objects* > *Web Filter* > *Web URL Filter*.

2 In the Content Pane, select the name *of* a URL filter.

3 Select *Create New*.

4 Complete the following:

Entry	The name of this entry. This is read only.
URL	Enter the URL. Do not include http://.
Type	Select a filter type from the dropdown list: Wildcard or regular Expression.

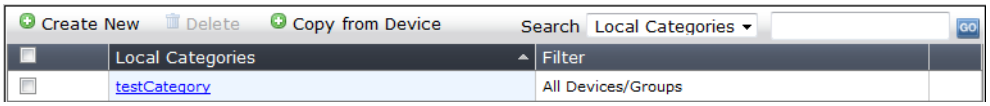
Action	Select an action from the dropdown list: *Allow*, *Block*, or *Exempt*.
Enable	Select to enable the URL.

5 Select *OK*.

Configuring local categories

User-defined categories can be created to allow users to block groups of URLs on a per-profile basis. The categories defined here appear in the global URL category list when configuring a protection profile. Users can rate URLs based on the local categories.

Figure 99: Local category list



Create New	Select to add a new local category. For more information, see "To add a local category" on page 152.
Delete	Select the check box beside a local category that you want to delete, then select *Delete* to remove it. You cannot delete the local category if it is included in a protection profile.
Copy from Device	Select to import a local category from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the local category list. Select *Local Categories* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a category in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Local Categories	The available local categories. Select to view or edit a category.
Filter	EMS mode only. Display the devices and groups that can use the global local category configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add a local category

1 Go to Local Category. In EMS mode, go to *Global Objects* > *Policy Objects* > *Web Filter* > *Local Category*. In GMS mode, go to *Security Console* > *Policy Objects* > *Web Filter* > *Local Category*.

2 In the Content Pane, select *Create New*.

Category Description	Enter a name to identify the local category.
Traffic Priority	Select *High*, *Medium*, or *Low*. Select *Traffic Priority* so the device manages the relative priorities of different types of traffic. For example, a policy for connecting to a secure web server needed to support e-commerce traffic should be assigned a high traffic priority. Less important services should be assigned a low priority. The firewall provides bandwidth to low-priority connections only when bandwidth is not needed for high-priority connections.

Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global local category configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global local category configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.

3 Select *OK*.

Configuring global spam filters

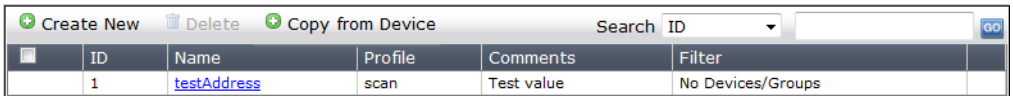
You can configure spam filters to be used in firewall protection profiles to stop unsolicited commercial email.

For more information about anti-spam filters, see the FortiGate documentation.

Configuring IP addresses

You can add antispam IP addresses to be included in a protection profile.

Figure 100: IP address list



Create New	Select to add a new IP address. For more information, see "To add an IP address" on page 153.
Delete	Select the check box beside an IP address that you want to delete, then select *Delete* to remove it. You cannot delete the IP address if it is included in a protection profile.
Copy from Device	Select to import an IP address from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the IP address list. Select *ID*, *Name,* or *Comment* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of an address in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
ID	The unique identification number of the IP address.
Name	The available IP addresses. Select a name to view or edit.
Profile	The protection profiles each IP address has been applied to.
Comments	Optional description of each IP address.
Filter	EMS mode only. Display the devices and groups that can use the global IP address configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add an IP address

1 Go to IP Address. In EMS mode, go to *Global Objects* > *Policy Objects* > *Anti-Spam* > *IP Address*. In GMS mode, go to *Security Console* > *Policy Objects* > *Anti-Spam* > *IP Address*.

2 in the Content Pane, select *Create New*.

3 Enter the name of the new IP address.

4 Enter a comment to describe the IP address, if required.

5 Select *Apply*.

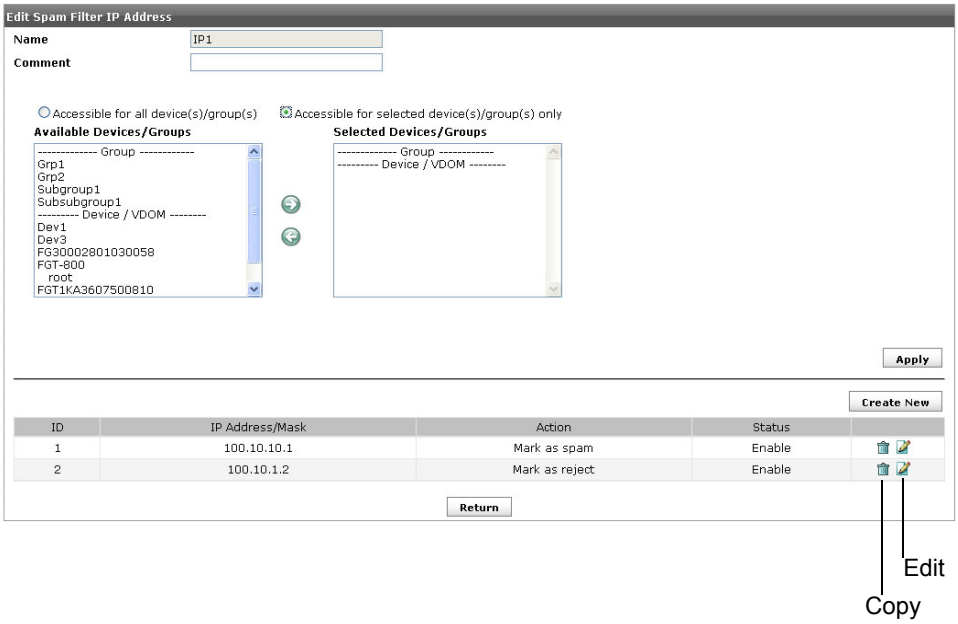
The new IP address appears on the IP address list.

To view or edit the IP address

1 Go to IP Address. In EMS mode, go to *Global Objects* > *Policy Objects* > *Anti-Spam* > *IP Address*. In GMS mode, go to *Security Console* > *Policy Objects* > *Anti-Spam* > *IP Address*.

2 In the Content Pane, select the *Edit* for the IP address to view or edit.

Figure 101: IP address



To add the IP address filter

1 Go to IP Address. In EMS mode, go to *Global Objects* > *Policy Objects* > *Anti-Spam* > *IP Address*. In GMS mode, go to *Security Console* > *Policy Objects* > *Anti-Spam* > *IP Address*.

2 Select the name of an IP address.

3 Select *Create New*.

4 Complete the following:

IP Address/Mask	Enter the IP address or the IP address/mask pair.
Action	Select: *Mark as Spam* to apply the spam action configured in the protection profile; *Mark as Clear* to bypass this and remaining spam filters; or *Mark as Reject (SMTP only)* to drop the session.
Enable	Select to enable the address.

5 Select *OK*.

Configuring email addresses

You can add antispam email addresses to be included in a protection profile.

To view the antispam email address list, in EMS mode, go to *Global Objects* > *Policy Objects* > *Anti-Spam* > *Email Address*. In GMS mode, go to *Security Console* > *Policy Objects* > *Anti-Spam* > *Email Address*.

Figure 102: Email address list

Create New	Select to add a new email address. For more information, see "To add an email address" on page 155.
Delete	Select the check box beside an email address that you want to delete, then select *Delete* to remove it. You cannot delete the email address if it is included in a protection profile.
Copy from Device	Select to import an email address from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the email address list. Select *ID*, *Name,* or *Comment* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of an address in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
ID	The unique identification number of the email address.
Name	The available email addresses. Select a name to view or edit.
Profiles	The protection profiles each email address list has been applied to.
Comment	Optional description of each email address list.
Filter	EMS mode only. Display the devices and groups that can use the global email address configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "To view or edit the email address" on page 156.

To add an email address

1. Go to Email Address. In EMS mode, go to *Global Objects* > *Policy Objects* > *Anti-Spam* > *Email Address*. In GMS mode, go to *Security Console* > *Policy Objects* > *Anti-Spam* > *Email Address*.
2. In the Content Pane, select *Create New*.
3. Enter the name of the new email address.
4. Enter a comment to describe the email address, if required.
5. Select *Apply*.

   The new email address appears on the email address list.

To view or edit the email address

1 Do one of the following:

- In EMS mode, go to *Global Objects* > *Policy Objects* > *Anti-Spam* > *Email Address*.
- In GMS mode, go to *Security Console* > *Policy Objects* > *Anti-Spam* > *Email Address*.

2 Select the name of the email address you want to view or edit.

3 Complete the following:

Name	Email address name. This is read-only.
Comments	Optional comment. To add or edit comment, enter text and select *Apply*.
Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global email address configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global email address configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.
Create New	Select to add a new email address filter to the email address.
Checkbox	Select the checkbox of an address in the list, and right-click to delete, edit, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
ID	The identification numbers of the email address filters.
Email address	The list of email addresses.
Pattern Type	The pattern type used in the email address filter.
Action	The action to take on email from the configured address. Actions are: *Spam* to apply the spam action configured in the protection profile, or *Clear* to let the email message bypass this and remaining spam filters.
Status	Display if the email address filter is activated.

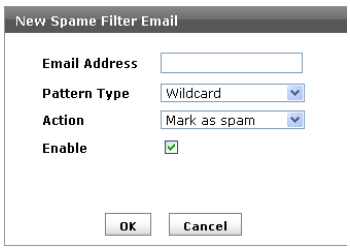
To add the email address filter

1 Go to Email Address. In EMS mode, go to *Global Objects* > *Policy Objects* > *Anti-Spam* > *Email Address*. In GMS mode, go to *Security Console* > *Policy Objects* > *Anti-Spam* > *Email Address*.

2 In the Content Pane, select the name of an email address.

3 Select *Create New*.

Figure 103: New email address



4 Complete the following:

Email Address	Enter the email address.
Pattern Type	Select a filter pattern type: *Wildcard* or *Regular Expression*.
Action	Select: *Mark as Spam* to apply the spam action configured in the protection profile, or *Mark as Clear* to bypass this and remaining spam filters.
Enable	Select to enable the email address for spam checking.

5 Select *OK*.

Configuring banned words

You can add antispam banned words to be included in a protection profile.

Figure 104: Email banned word list

Create New	Select to add a new banned word. For more information, see "To add a banned word list" on page 157.
Delete	Select the check box beside a banned word that you want to delete, then select *Delete* to remove it. You cannot delete the banned word if it is included in a protection profile.
Copy from Device	Select to import a banned word from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the banned word list. Select *ID*, *Name,* or *Comment* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a word in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
ID	The unique identification number of the banned word.
Name	The available banned words. Select to view or edit a banned word.
Profile	The protection profiles each banned word has been applied to.
Comments	Optional description of each banned word.
Filter	EMS mode only. Display the devices and groups that can use the global banned word configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add a banned word list

1 Go to Banned Word. In EMS mode, go to *Global Objects* > *Policy Objects* > *Anti-Spam* > *Banned Word*. In GMS mode, go to *Security Console* > *Policy Objects* > *Anti-Spam* > *Banned Word*.

2 In the Content Pane, select *Create New*.

3 Enter the name of the new banned word.

4 Enter a comment to describe the banned word, if required.

5 Select *Apply*.

The new banned word appears on the banned word list.

To view or edit the banned word list

1 Go to Banned Word. In EMS mode, go to *Global Objects* > *Policy Objects* > *Anti-Spam* > *Banned Word*. In GMS mode, go to *Security Console* > *Policy Objects* > *Anti-Spam* > *Banned Word*.

2 In the Content Pane, select the *Edit* icon of the banned word to view or edit.

3 Complete the following:

Name	Banned word name. This is read-only.
Comments	Optional comment. To add or edit comment, enter text and select *Apply*.
Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global banned word configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global banned word configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.
Create New	Select to add a new banned word entry to the banned word list.
Checkbox	Select the checkbox of an address in the list, and right-click to delete, edit, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
ID	The identification numbers of the banned word entries.
Pattern	The list of banned word entries.
Pattern Type	The pattern type used in the banned word entry.
Language	The character set to which the banned word belongs.
Where	The location from where the banned word is searched: *Subject*, *Body*, or *All*.
Action	Select: *Mark as Spam* to apply the spam action configured in the protection profile, or *Mark as Clear* to bypass this and remaining spam filters.
Score	A numerical weighting applied to the banned word. The score values of all the matching words appearing in an email message are added, and if the total is greater than the Banned word check value set in the protection profile, the email is processed according to whether the spam action is set to Discard or Tagged in the protection profile. The score for a banned word is counted once even if the word appears multiple times on the web page in the email.
Status	Display if the banned word entry is activated.

To add a banned word entry

1 Go to Banned Word. In EMS mode, go to *Global Objects* > *Policy Objects* > *Anti-Spam* > *Banned Word*. In GMS mode, go to *Security Console* > *Policy Objects* > *Anti-Spam* > *Banned Word*.

2 In the Content Pane, select the name of a banned word.

3 Select *Create New*.

4 Complete the following:

Expression	Enter the word or phrase you want to include in the banned word.
Pattern Type	Select the pattern type for the banned word. Choose from wildcard or regular expression.
Language	Select the character set for the banned word.
Where	Select the location from where the banned word is searched: *Subject*, *Body*, or *All*.
Action	Select: *Mark as Spam* to apply the spam action configured in the protection profile, or *Mark as Clear* to bypass this and remaining spam filters.
Score	A numerical weighting applied to the banned word. The score values of all the matching words appearing in an email message are added, and if the total is greater than the banned word check value set in the protection profile, the email is processed according to whether the spam action is set to *Discard* or *Tagged* in the protection profile. The score for a banned word is counted once even if the word appears multiple times on the web page in the email.
Enable	Select to enable scanning for the banned word.

5 Select *OK*.

Configuring SSL VPN portal

You can import an SSL VPN portal configuration from a device. You cannot modify the imported SSL VPN portal configuration.

To import an SSL VPN portal configuration, create SSL VPN portals on the device first and then go to SSL VPN Portal copy from device.

In EMS mode, go to *Global Objects* > *Policy Objects* > *SSL VPN Portal* > *Copy from Device*.

In GMS mode, go to *Security Console* > *Policy Objects* > *SSL VPN Portal* > *Copy from Device*.

For information on creating SSL VPN portals, see the *FortiGate Administration Guide* and the *SSL VPN User Guide*.

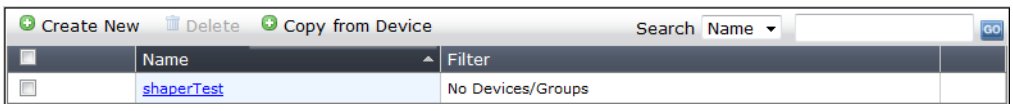
•

Configuring traffic shaping (EMS mode)

Traffic shaping controls the bandwidth available to, and sets the priority of the traffic processed by, the firewall policy. Traffic shaping makes it possible to control which policies have the highest priority when large amounts of data are moving through the device.

Traffic shaping cannot increase the total amount of bandwidth available, but you can use it to improve the quality of bandwidth-intensive and sensitive traffic.

Figure 105: Traffic shaper list



Create New	Select to add a new traffic shaper. For more information, see "To add a traffic shaper" on page 160.
Delete	Select the check box beside a traffic shaper that you want to delete, then select *Delete* to remove it.
Copy from Device	Select to import a traffic shaper from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.

Search	Search the traffic shaper list. Select *Name* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a traffic shaper in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The available traffic shapers. Select to view or edit a traffic shaper.
Filter	EMS mode only. Display the devices and groups that can use the global traffic shaping configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add a traffic shaper

1 In EMS mode, go to *Global Objects* > *Policy Objects* > *Traffic Shaping*.

2 In the Content Pane, select *Create New*.

3 Complete the following:

Name	Enter a name to identify the traffic shaper.
Apply Shaping	Select *Per Policy* to apply this traffic shaper to a single firewall policy that uses it. Select *For all policies using this shaper* to apply this traffic shaper to all firewall policies that use it.
Guaranteed Bandwidth	Enter a value (0 - 2097000) to ensure there is enough bandwidth available for a high-priority service. Be sure that the sum of all *Guaranteed Bandwidth* in all firewall policies is significantly less than the bandwidth capacity of the interface.
Maximum Bandwidth	Enter a value (0 - 2097000) to limit bandwidth in order to keep less important services from using bandwidth needed for more important ones.
Traffic Priority	Select *High*, *Medium*, or *Low*. Select *Traffic Priority* so the device manages the relative priorities of different types of traffic. For example, a policy for connecting to a secure web server needed to support e-commerce traffic should be assigned a high traffic priority. Less important services should be assigned a low priority. The firewall provides bandwidth to low-priority connections only when bandwidth is not needed for high-priority connections.
Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global traffic shaping configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global traffic shaping configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.

4 Select *OK*.

Configuring user authentication

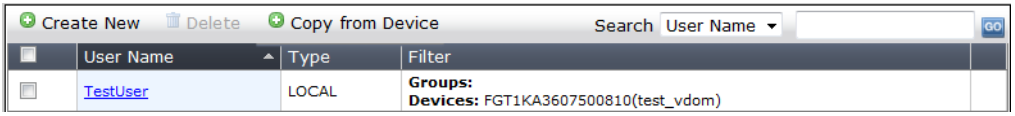
Set up user accounts, user groups, and external authentication servers. You can use these components of user authentication to control access to network resources.

Configuring local user accounts

A local user is a user configured on a device. The user can be authenticated with a password stored on the device (the user name and password must match a user account stored on the device) or with a password stored on an authentication server (the user name must match a user account stored on the device and the user name and password must match a user account stored on the authentication server associated with the user).

To view the local user list, go to *Global Objects* > *Policy Objects* > *User Authentication* > *Local*.

Figure 106: Firewall local user list



Create New	Select to add a user. For more information, see "To add a local user" on page 161.
Delete	Select the check box beside a local user that you want to delete, then select *Delete* to remove the user. You cannot delete the user if it is included in a user group.
Copy from Device	Select to import a local user from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the local user list. Select *User Name* or *Type* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a user in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
User Name	The name of the local user. Select to view or edit a user.
Type	The authentication type to use for this user. The authentication types are Local (user and password stored on FortiGate unit), LDAP, RADIUS, and TACACS+ (user and password matches a user account stored on the authentication server).
Filter	EMS mode only. Display the devices and groups that can use the global local user configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add a local user

1. Go to Local. In EMS mode, go to *Global Objects* > *Policy Objects* > *User Authentication* > *Local*. In GMS mode, go to *Security Console* > *Policy Objects* > *User Authentication* > *Local*.
2. In the Content Pane, select *Create New*.
3. Complete the following:

User Name	Enter a name for the local user.

Disable **Password** **LDAP** **RADIUS** **TACACS+**	See the FortiGate documentation for complete information on completing these options.
Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global local user configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global local user configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.

4 Select *OK*.

The new local user appears on the local user list.

Configuring RADIUS servers

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

For more information about RADIUS servers, see the FortiGate documentation.

Figure 107: RADIUS server list

Create New	Select to add a RADIUS server. For more information, see "To add a RADIUS server" on page 163.
Delete	Select the check box beside a RADIUS server that you want to delete, then select *Delete* to remove the server. You cannot delete the server if it belongs to a user group or is chosen by a local user as an authentication type.
Copy from Device	Select to import a RADIUS server from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the RADIUS server list. Select *Name* or *Server Name/IP* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a server in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name that identifies the RADIUS server. Select to view or edit a server.

Server Name/IP	The domain name or IP address of the RADIUS server.
Filter	EMS mode only. Display the devices and groups that can use the global RADIUS server configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add a RADIUS server

1 Go to RADIUS. In EMS mode, go to *Global Objects* > *Policy Objects* > *User Authentication* > *RADIUS*. In GMS mode, go to *Security Console* > *Policy Objects* > *User Authentication* > *RADIUS*.

2 In the Content Pane, select *Create New*.

3 Complete the following:

Name **Primary Server Name/IP** **Primary Server Secret** **Secondary Server Name/IP** **Secondary Server Secret** **Authentication Scheme** **NAS IP** **All User Group**	See the FortiGate documentation for complete information on completing these options.
Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global RADIUS server configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global RADIUS server configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.

4 Select *Ok*.

The new RADIUS server appears on the RADIUS server list.

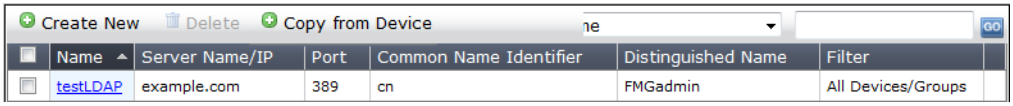
Configuring LDAP servers

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. An LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

For more information about LDAP servers, see the FortiGate documentation.

To view the LDAP server list, go to *Global Objects* > *Policy Objects* > *User Authentication* > *LDAP*.

Figure 108: LDAP server list



Create New	Select to add a LDAP server. For more information, see "To add an LDAP server" on page 164.
Delete	Select the check box beside a LDAP server that you want to delete, then select *Delete* to remove the server. You cannot delete the server if it belongs to a user group or is chosen by a local user as an authentication type.
Copy from Device	Select to import a LDAP server from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the LDAP server list. Select *Name, Server Name/IP, Port, Common Name Identifier, or Distinguished Name* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a server in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name that identifies the LDAP server. Select to view or edit a server.
Server Name/IP	The domain name or IP address of the LDAP server.
Port	The TCP port used to communicate with the LDAP server.
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.
Filter	EMS mode only. Display the devices and groups that can use the global LDAP server configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add an LDAP server

1 Go to LDAP. In EMS mode, go to *Global Objects* > *Policy Objects* > *User Authentication* > *LDAP*. In GMS mode, go to *Security Console* > *Policy Objects* > *User Authentication* > *LDAP*.

2 In the Content Pane, select *Create New*.

3 Complete the following:

Name **Server Name/IP** **Server Port** **Common Name Identifier** **Distinguished Name** **Bind Type** **Secure Connection**	See the FortiGate documentation for complete information on completing these options.
Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global LDAP server configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global LDAP server configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.

4 Select *OK*.

The new LDAP server appears on the LDAP server list.

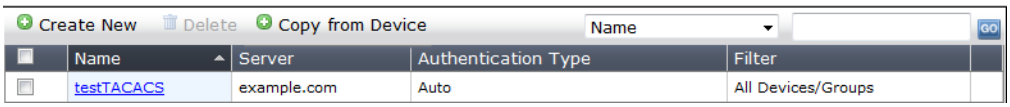
Configuring TACACS servers

In recent years, remote network access has shifted from terminal access to LAN access. Users connect to their corporate network (using notebooks or home PCs) with computers that use complete network connections and have the same level of access to the corporate network resources as if they were physically in the office. These connections are made through a remote access server. As remote access technology has evolved, the need for network access security has become increasingly important.

Terminal Access Controller Access-Control System (TACACS) is a remote authentication protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. 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 more information about TACACS servers, see the FortiGate documentation.

Figure 109: TACACS server list



Create New	Select to add a TACACS server. For more information, see "To add a TACACS server" on page 166.
Delete	Select the check box beside a TACACS server that you want to delete, then select *Delete* to remove the server. You cannot delete the server if it belongs to a user group or is chosen by a local user as an authentication type.
Copy from Device	Select to import a TACACS server from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.

Search	Search the TACACS server list. Select *Name, Server, or Authentication Type* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a server in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name that identifies the TACACS server. Select to view or edit a server.
Server	The domain name or IP address of the TACACS server.
Authentication Type	The supported authentication method. TACACS authentication methods include: Auto, ASCII, PAP, CHAP, and MSCHAP.
Filter	EMS mode only. Display the devices and groups that can use the global TACACS server configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add a TACACS server

1 Go to TACACS. In EMS mode, go to *Global Objects* > *Policy Objects* > *User Authentication* > *TACACS*. In GMS mode, go to *Security Console* > *Policy Objects* > *User Authentication* > *TACACS*.

2 In the Content Pane, select *Create New*.

3 Complete the following:

Name	Enter the name of the TACACS server.
Server Name/IP	Enter the server domain name or IP address of the TACACS server.
Server Key	Enter the key to access the TACACS server. The maximum number is 16.
Authentication Type	Select the authentication type to use for the TACACS server. Selection includes: Auto, ASCII, PAP, CHAP, and MSCHAP. Auto authenticates using PAP, MSCHAP, and CHAP (in that order).
Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global TACACS server configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global TACACS server configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.

4 Select *OK*.

The new TACACS server appears on the TACACS server list.

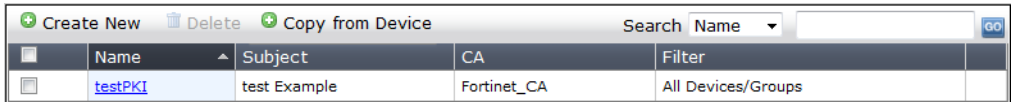
Configuring PKI authentication

Public Key Infrastructure (PKI) authentication utilizes a certificate authentication library that takes a list of peers, peer groups, and/or user groups and returns authentication successful or denied notifications. Users only need a valid certificate for successful authentication—no user name or password are necessary. Firewall and SSL VPN are the only user groups that can use PKI authentication.

For more information about PKI authentication, see the FortiGate documentation.

To view the list of PKI users, go to *Global Objects* > *Policy Objects* > *User Authentication* > *PKI*.

Figure 110: PKI User list



Create New	Select to add a PKI user. For more information, see "To add a PKI user" on page 167.
Delete	Select the check box beside a PKI user that you want to delete, then select *Delete* to remove the user. You cannot delete the user if it belongs to a user group.
Copy from Device	Select to import a PKI user from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the PKI user list. Select *Name, Subject, or CA* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of an entry in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name of the PKI user. Select to view or edit a user.
Subject	The text string that appears in the subject field of the certificate of the authenticating user.
CA	The CA certificate that is used to authenticate this user.
Filter	EMS mode only. Display the devices and groups that can use the global PKI authentication configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add a PKI user

1. Go to PKI. In EMS mode, go to *Global Objects* > *Policy Objects* > *User Authentication* > *PKI*. In GMS mode, go to *Security Console* > *Policy Objects* > *User Authentication* > *PKI*.
2. In the Content Pane, select *Create New*.
3. Complete the following:

Name	Enter the name of the PKI user.
Subject	Enter the text string that appears in the subject field of the certificate of the authenticating user. This field is optional.
CA	Enter the CA certificate that must be used to authenticate this user. This field is optional.

Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global PKI authentication configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global PKI authentication configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.

4 Select *OK*.

The new PKI user appears on the PKI user list.

Configuring user groups

A user group is a list of user identities. An identity can be:

- a local user account (user name and password) stored on the Fortinet unit
- a local user account with a password stored on a RADIUS, LDAP, or TACACS+ server
- a RADIUS, LDAP, or TACACS+ server (all identities on the server can authenticate)
- a user or user group defined on a Directory Service server.

  Each user group belongs to one of three types: Firewall, Directory Service or SSL VPN.

For more information about user groups, see the FortiGate documentation.

Figure 111: User group list

Create New	Select to add a user group. For more information, see "To add a user group" on page 169.
Delete	Select the check box beside a user group that you want to delete, then select *Delete* to remove the user. You cannot delete a user group that is included in a firewall policy, a dialup user phase 1 configuration, or a PPTP or L2TP configuration.
Copy from Device	Select to import a user group from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the user group list. Select *Group Name, Type, or Protection Profile* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of an entry in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Group Name	The name of the user group.
Type	The type of user groups. For example, *Firewall* and *Active Directory*. For more information, see the *FortiGate Administration Guide*.
Members	The Local users, RADIUS servers, LDAP servers, TACACS servers, Directory Service users/user groups or PKI users found in the user group.

Protection Profile	The protection profile associated with this user group.
Filter	EMS mode only. Display the devices and groups that can use the global user group configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add a user group

1 Go to User Group. In EMS mode, go to *Global Objects* > *Policy Objects* > *User Authentication* > *User Group*. In GMS mode, go to *Security Console* > *Policy Objects* > *User Authentication* > *User Group*.

2 In the Content Pane, select *Create New*.

3 Complete the following information:

Group Name	Enter the name of the user group.
Type **Protection Profile** **Available Users/Groups** **Members** **FortiGuard Web Filtering Override**	See the FortiGate documentation for complete information on completing these options.
Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global user group configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global user group configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.

4 Select *OK*.

The new user group appears on the user group list.

Configuring load balancing

Configure device load balancing to intercept the incoming traffic and share it across the available servers. By doing so, a device can enable multiple servers to respond as if they were a single device or server. This in turn means that more simultaneous requests can be handled.

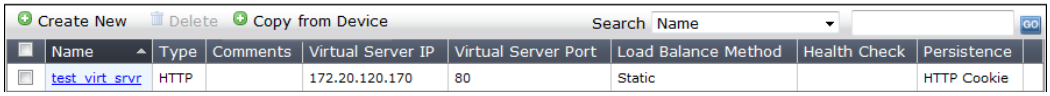
There are additional benefits to server load balancing. Firstly, because the sessions load is distributed across multiple servers, the service being provided can be highly available. If one of the servers breaks down, the load can still be handled by the other servers. Secondly, this increases scalability. If the load increases substantially, more servers can be added behind the device in order to cope with the increased load.

To configure load balancing, configure virtual servers, real servers, and health check monitors.

Configuring virtual servers (GMS mode)

Configure a virtual server's external IP address and bind it to a device's interface. When you bind the virtual server's external IP address to a device's interface, by default, the network interface responds to ARP requests for the bound IP address. Virtual servers use proxy ARP, as defined in RFC 1027, so that the device can respond to ARP requests on a network for a real server that is actually installed on another network. To disable ARP replies, see the *FortiGate CLI Reference*.

Figure 112: Virtual server list



Create New	Select to add a virtual server. For more information, see "To add a health check monitor" on page 173.
Delete	Select the check box beside a virtual server that you want to delete, then select *Delete* to remove the server. You cannot delete a server that is included in a firewall policy.
Copy from Device	Select to import a virtual server from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Checkbox	Select the checkbox of an entry in the list, and right-click to delete, edit, clone, copy, clear up, query device database(s), search, or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	Name of the virtual server.
Type	The communication protocol used by the virtual server.
Comments	Comments on the virtual server.
Virtual Server IP	The IP address of the virtual server.
Virtual server Port	The port number to which the virtual server communicates.
Load Balance Method	Load balancing methods include: • *Static*: The traffic load is spread evenly across all servers, no additional server is required. • *Round Robin*: Directs requests to the next server, and treats all servers as equals regardless of response time or number of connections. Dead servers or non responsive servers are avoided. A separate server is required. • *Weighted*: Servers with a higher weight value will receive a larger percentage of connections. Set the server weight when adding a server. • *First Alive*: Always directs requests to the first alive real server. First alive means that if you configure servers A, B, and C in that order in the CLI, then traffic will always go to A as long as it is alive. If and when A goes down then traffic will go to B and if B goes down the traffic will go to C. "First" refers to the order of the servers in the CLI configuration. • *Least RTT*: Directs requests to the server with the least round trip time. The round trip time is determined by a Ping monitor and is defaulted to 0 if no Ping monitors are defined. • *Least Session*: Directs requests to the server that has the least number of current connections. This method works best in environments where the servers or other equipment you are load balancing have similar capabilities.

Health Check	The health check monitor selected for this virtual server. For more information, see "Health Check" on page 171.
Persistence	Persistence is the process of ensuring that a user is connected to the same server every time they make a request within the boundaries of a single session. Depending on the type of protocol selected for the virtual server, the following persistence options are available: • *None*: No persistence option is selected. • *HTTP Cookie*: Persistence time is equal to the cookie age. Cookie ages are set in CLI under `config firewall vip`. • SSL Session ID: Persistence time is equal to the SSL sessions. SSL session states are set in CLI under `config firewall vip`.

To add a virtual server

1 In GMS mode, go to *Security Console* > *Policy Objects* > *Load Balance* > *Virtual Server*.

2 In the Content Pane, select *Create New*.

3 Complete the following:

Name	Enter the name for the virtual server.
Type	Enter the communication protocol used by the virtual server.
Interface	Select the virtual server external interface from the list. The external interface is connected to the source network and receives the packets to be forwarded to the destination network.
Virtual Server IP	Enter the IP address of the virtual server.
Virtual server Port	The port number to which the virtual server communicates.
Load Balance Method	Select a load balancing method as one of Static, Round Robin, Weighted, Least Session, Least Round Trip Time (RTT), or First Alive.
Persistence	Select a persistence for the virtual server. For more information, see "Persistence" on page 171.
HTTP Multiplexing	Select to use the device's HTTP proxy to multiplex multiple client connections destined for the web server into a few connections between the device and the web server. This can improve performance by reducing server overhead associated with establishing multiple connections. The server must be HTTP/1.1 compliant. This option appears only if *HTTP* is selected for *Type*. **Note**: Additional HTTP Multiplexing options are available in the CLI. For more information, see the *FortiGate CLI Reference*.
Preserve Client IP	Select to preserve the IP address of the client in the `X-Forwarded-For` HTTP header. This can be useful if you require logging on the server of the client's original IP address. If this option is not selected, the header will contain the IP address of the FortiGate unit. This option appears only if *HTTP* is selected for *Type*, and is available only if *HTTP Multiplexing* is selected.
Health Check	Select which health check monitor configuration will be used to determine a server's connectivity status. For information on configuring health check monitors, see "Configuring health check monitors" on page 172.
Comments	Any comments or notes about this virtual server.

4 Select *OK*.

Configuring real servers (GMS mode)

Configure a real server to bind it to a virtual server.

The Real Server list fields include:

Create New	Select to add real servers. For more information, see "To add a real server" on page 172.
IP Address	Select the blue arrow beside a virtual server name to view the IP addresses of the real servers that are bound to it.
Port	The port number on the destination network to which the external port number is mapped.
Weight	The weight value of the real server. The higher the weight value, the higher the percentage of connections the server will handle.
Max Connection	The limit on the number of active connections directed to a real server. If the maximum number of connections is reached for the real server, the device will automatically switch all further connection requests to another server until the connection number drops below the specified limit.

To add a real server

1 In GMS mode, go to *Security Console* > *Policy Objects* > *Load Balance* > *Real Server*.

2 In the Content Pane, select *Create New*.

3 Complete the following:

Virtual Server	Select the virtual server to which you want to bind this real server.
IP Address	Enter the IP address of the real server.
Port	Enter the port number on the destination network to which the external port number is mapped.
Weight	Enter the weight value of the real server. The higher the weight value, the higher the percentage of connections the server will handle. A range of 1-255 can be used. This option is available only if the associated virtual server's load balance method is *Weighted*.
Max Connection	Enter the limit on the number of active connections directed to a real server. A range of 1-99999 can be used. If the maximum number of connections is reached for the real server, the device will automatically switch all further connection requests to another server until the connection number drops below the specified limit.

4 Select *OK*.

Configuring health check monitors

Health check monitor configurations are used to determine a server's connectivity status.

Health check monitor configurations can specify TCP, HTTP or ICMP PING. A health check occurs every number of seconds indicated by the interval. If a reply is not received within the timeout period, and you have configured the health check to retry, it will attempt a health check again; otherwise, the server is deemed unresponsive, and load balancing will compensate by disabling traffic to that server until it becomes responsive again.

Figure 113: Health check monitor list

Create New	Select to add a health check monitor. For more information, see "To add a health check monitor" on page 173.
Copy from Device	Select to import a health check monitor from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
TCP **HTTP** **PING**	Select the arrow next to TCP, HTTP, or PING to expand the list of that type of monitors. Beside each type of monitor is the number of entries in brackets.
Checkbox	Select the checkbox of one or more entries and right-click to delete, edit, clone, copy, clear up, query device database(s) or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name of the health check monitor configuration. The names are grouped by the health check monitor types.
Details	The details of the health check monitor configuration, which vary by the type of the health check monitor, and do not include the interval, timeout, or retry, which are settings common to all types. This field is empty if the type of the health check monitor is PING.
Filter	EMS mode only. Display the devices and groups that can use the global user group configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "Accessibility options - EMS mode" on page 129.

To add a health check monitor

1 Do one of the following:

- In EMS mode, go to *Global Objects* > *Policy Objects* > *Load Balance* > *Health Check Monitor*.
- In GMS mode, go to *Security Console* > *Policy Objects* > *Health Check Monitor*.

2 Select *Create New*.

Name	Enter the name of the health check monitor configuration.
Type	Select the protocol used to perform the health check. • TCP • HTTP • PING
Port	Enter the port number used to perform the health check. This option does not appear if the *Type* is *PING*.
URL	Enter the URL that will receive the HTTP request. This option appears only if *Type* is *HTTP*.
Matched Content	Enter the HTTP reply content that must be present to indicate proper server connectivity. This option appears only if *Type* is *HTTP*.
Interval	Enter the number of seconds between each server health check.
Timeout	Enter the number of seconds which must pass after the server health check to indicate a failed health check.
Retry	Enter the number of times, if any, a failed health check will be retried before the server is determined to be inaccessible.

Accessible for all device(s)/group(s)	EMS mode only. Select to allow all devices or groups to use the global health check monitor configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	EMS mode only. Select to allow selected devices or groups to use the global health check monitor configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.

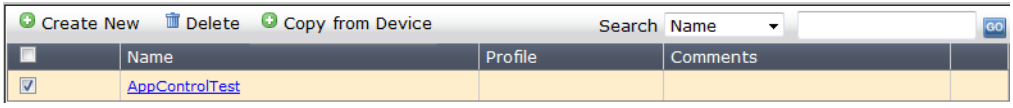
3 Select *OK*.

Configuring application control list

Application control is a UTM feature that allows your FortiGate unit to detect and take action against network traffic depending on the application generating the traffic. Based on FortiGate Intrusion Protection (IPS) protocol decoders, application control is a more user-friendly and powerful way to use IPS features to log and manage the behavior of application traffic passing through the FortiGate unit. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols.

The FortiGate unit can recognize the network traffic generated by more than 70 applications. You can create application control lists that specify what action will be taken with the traffic of the applications you need to manage. Specify the application control list in the protection profile applied to the network traffic you need to monitor. Create multiple application control lists, each tailored to a particular network, for example.

Figure 114: Application control list



Create New	Select to add an application control list. For more information, see "To add an application control list" on page 174.
Delete	Select the check box beside an application control list that you want to delete, then select *Delete* to remove it. You cannot delete an application control list that is used by a protection profile.
Copy from Device	Select to import an application control configuration from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the application control list. Select *Name or Comment* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of one or more entries and right-click to delete, edit, clone or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name that identifies the application control list. Select to view or edit an application control list.
# of Entries	The number of application rules in each application control list.
Profile	The protection profile each application control list has been applied to. If the list has not been applied to a protection profile, this field will be blank.
Comments	An optional description of each application control list.

To add an application control list

1 In GMS mode, go to *Security Console* > *Policy Objects* > *Control List*.

2 In the Content Pane, select *Create New*.
3 Enter the name for the application control list.
4 Optionally, enter any comments for the application control list.
5 Select *Apply*.

To view or edit an application control list

1 In GMS mode, go to *Security Console* > *Policy Objects* > *Control List*.
2 In the Content Pane, select the name of the application control list you want to view or edit.

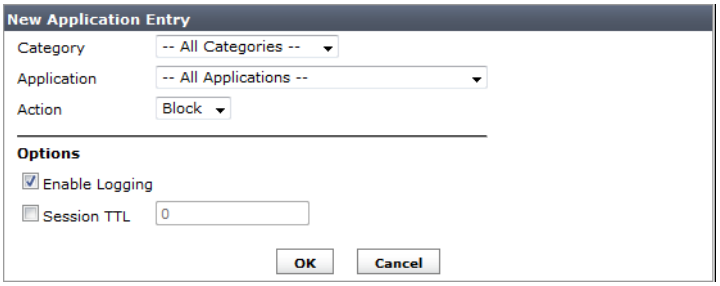
Name	The name of the application control list.
Comment	Enter or edit a comment about the list. The comment is optional.
List Type	Select one of Black List or White List. Black List allows all undefined applications, and White List denies all undefined applications.
Enable log for other applications	Select to enable logging.
Apply	Select to save any modifications made to the application control list.
Create New	Select to create a new application entry. See "To add an application control list entry" on page 175.
Checkbox	Select the checkbox of one or more entries and right-click to delete, edit, insert, move or select all. For more on the right-click menu, see "Right-click menu" on page 126.
ID	A unique number used primarily when re-ordering application entries.
Category	The category indicates the scope of the applications included in the application entry if *Application* is set to *all*. For example, if *Application* is *all* and *Category* is *toolbar*, then all the toolbar applications are included in the application entry even though they are not specified individually. If *Application* is a single application, the value in *Category* has no effect on the operation of the application entry.
Application	The FortiGate unit will examine network traffic for the listed application. If *Application* is *all*, every application in the selected category is included.
Action	If the FortiGate unit detects traffic from the specified application, the selected action will be taken.
Logging	If traffic from the specified application is detected, the FortiGate unit will log the occurrence and the action taken.

To add an application control list entry

1 In GMS mode, go to *Security Console* > *Policy Objects* > *Control List*.
2 In the Content Pane, select the name of an application control list.
3 On the edit screen for that control list, select *Create New* to create a new control list entry.

Figure 115: Adding an application control list entry

4 Complete the following information:



Category	The applications are categorized by type. If you want to choose an IM application, for example, select the *im* category, and the application list will show only the *im* applications. The *Category* selection can also be used to specify an entire category of applications. To select all IM applications for example, select the *im* category, and select *All Applications* as the application. This specifies all the IM applications with a single application control list entry.
Application	The FortiGate unit will examine network traffic for the listed application. If *Application* is *All Applications*, every application in the selected category is included.
Action	If the FortiGate unit detects traffic from the specified application, the selected action will be taken.
Options	
Session TTL	The application's session TTL. If this option is not enabled, the TTL defaults to the setting of the `config system session-ttl` CLI command.
Enable Logging	When enabled, the FortiGate unit will log the occurrence and the action taken if traffic from the specified application is detected.

In addition to these option, some IM applications and VoIP protocols have additional options:

IM Options	
Block Login	Select to prevent users from logging in to the selected IM system.
Block File Transfers	Select to prevent the sending and receiving of files using the selected IM system.
Block Audio	Select to prevent audio communication using the selected IM system.
Inspect Non-standard Port	Select to allow the FortiGate unit to examine non-standard ports for the IM client traffic.
Display content meta-information on the system dashboard	Select to include meta-information detected for the IM system on the FortiGate unit dashboard.
VoIP Options	
Limit Call Setup	Enter the maximum number of calls each client can set up per minute.
Limit REGISTER request	Enter the maximum number of register requests per second allowed for the firewall policy.
Limit INVITE request	Enter the maximum number of invite requests per second allowed for the firewall policy.
Enable Logging of Violations	Select to enable logging of violations.

5 Select *OK*.

Configuring data leak prevention

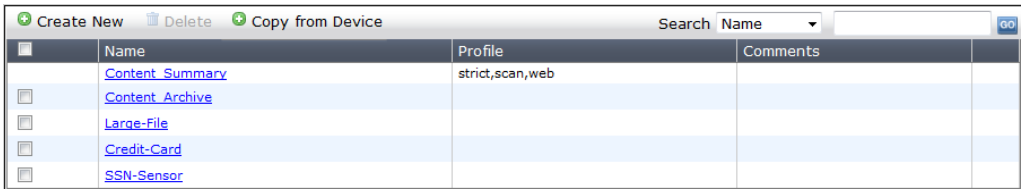
The FortiGate data leak prevention (DLP) system allows you to prevent sensitive data from leaving your network. You can define sensitive data patterns, and data matching these patterns will be blocked and/or logged when passing through the FortiGate unit. The DLP system is configured by creating individual rules, combining the rules into DLP sensors, and then assigning a sensor to a protection profile.

Although the primary use of the DLP feature is to stop sensitive data from leaving your network, it can also be used to prevent unwanted data from entering your network.

Configuring DLP sensors

DLP sensors are simply collections of DLP rules and DLP compound rules. Once a DLP sensor is configured, it can be specified in a protection profile. Any traffic handled by the policy in which the protection profile is specified will enforce the DLP sensor configuration.

Figure 116: DLP sensor list



Create New	Select to add a DLP sensor. For more information, see "To add a DLP sensor" on page 177.
Delete	Select the check box beside a DLP sensor that you want to delete, then select *Delete* to remove it. You cannot delete a DLP sensor that is used by a protection profile.
Copy from Device	Select to import a DLP sensor configuration from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the DLP sensor list. Select *Name, Comment, or Protection Profile* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of an entry in the list, and right-click to edit it. Select the checkbox of multiple groups in the list to delete, or clone the groups. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name that identifies the DLP sensor. Select to view or edit a DLP sensor.
Comments	An optional description of each DLP sensor.
Protection Profile	The names of the protection profiles in which the DLP sensor is used.

To add a DLP sensor

1. In GMS mode, go to *Security Console* > *Policy Objects* > *Data Leak Prevention* > *Sensor.*
2. In the Content Pane, select *Create New*.
3. Enter the name for the DLP sensor.
4. Optionally, enter any comments for the DLP sensor.
5. Select *Apply*.

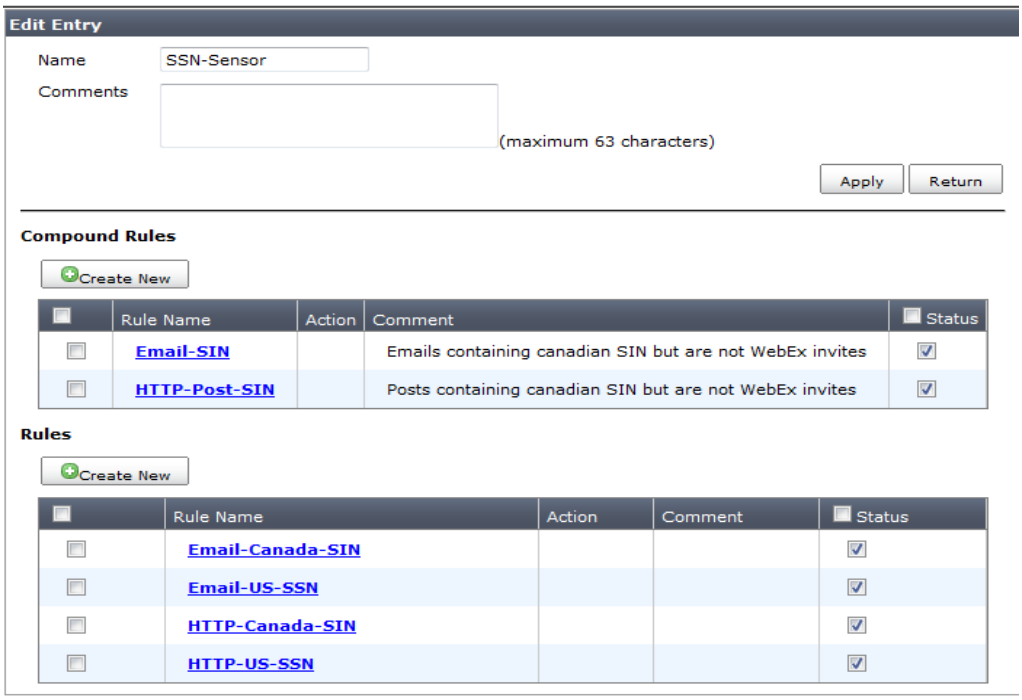
To view or edit a DLP sensor

1. Do one of the following:

2 In GMS mode, go to *Security Console* > *Policy Objects* > *Data Leak Prevention* > *Sensor.*

3 Select the name of the DLP sensor you want to view or edit.

Figure 117: Viewing or editing a DLP sensor



Name	The name of the DLP sensor.
Comment	Enter or edit a comment about the sensor. The comment is optional.
Apply	Select to save any modifications made to the DLP sensor.
Create New	Select to create a new DLP sensor entry.
Enable	You can disable a rule or compound rule by clearing this check box. The item will be listed as part of the sensor, but it will not be used.
Rule Name	The names of the rules and compound rules included in the sensor.
Action	The action configured for each rule. If the selected action is *None*, no action will be listed. Although archiving is enabled independent of the action, the *Archive* designation will appear with the selected action. For example, if you select the *Block* action and enable *Archive* for a rule, the action displayed in the sensor rule list is *Block, Archive*.
Comment	The optional description of the rule or compound rule.

To add a compound rule or rule in a DLP sensor

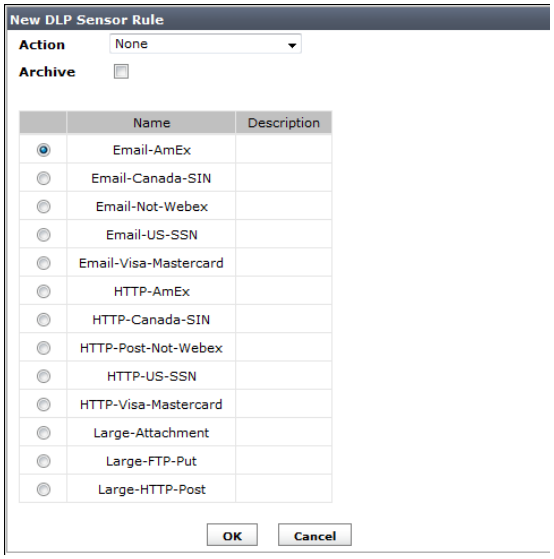
1 In GMS mode, go to *Security Console* > *Policy Objects* > *Data Leak Prevention* > *Sensor.*

2 Select the name of an existing DLP sensor to edit.

3 Under either Compound Rule or Rule, select *Create New*.

Figure 118: Adding a DLP sensor rule

4 Complete the following:



Action	Select the action to be taken against traffic matching the configured DLP rule or DLP compound rule. For more information about each action, see the *FortiGate Administration Guide*.
Archive	Content archive all traffic matching the DLP rule or compound rule. For more information about content archiving, see the *FortiGate Administration Guide*.

5 Select one Compound Rule or Rule from the list.

6 Select *OK*.

7 To add additional Compound Rules or Rules, repeat step 3 through step 6.

Configuring DLP compound rules

DLP compound rules are groupings of DLP rules that also change the way they behave when added to a DLP sensor. Individual rules can be configured with only a single attribute. When this attribute is discovered in network traffic, the rule is activated.

Compound rules allow you to group individual rules to specify far more detailed activation conditions. Each included rule is configured with a single attribute, but every attribute must be present before the rule is activated.

For example, create two rules and add them to a sensor:

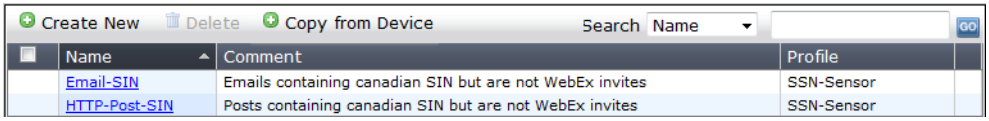
- Rule 1 checks SMTP traffic for a sender address of spammer@example.com
- Rule 2 checks SMTP traffic for the word “sale” in the message body

When the sensor is used, either rule could be activated its configured condition is true. If only one condition is true, only the corresponding rule would be activated. Depending on the contents of the SMTP traffic, neither, either, or both could be activated.

If you remove these rules from the sensor, add them to a compound rule, and add the compound rule to the sensor, the conditions in both rules have to be present in network traffic to activate the compound rule. If only one condition is present, the message passes without any rule or compound rule being activated.

By combining the individually configurable attributes of multiple rules, compound rules allow you to specify far more detailed and specific conditions to trigger an action.

Figure 119: DLP compound rule list



Create New	Select to add a compound rule. For more information, see "To add a compound rule" on page 180.
Delete	Select the check box beside a compound rule that you want to delete, then select *Delete* to remove it. You cannot delete a compound rule that is used by a DLP sensor.
Copy from Device	Select to import a compound rule configuration from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the compound rule list. Select *Name, Comment, or DLP Sensors* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of an entry in the list, and right-click to edit it. Select the checkbox of multiple groups in the list to delete, or clone the groups. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name that identifies the compound rule. Select to view or edit a compound rule.
Comment	An optional description of each compound rule.
Profile	If the compound rule is used in any sensors, the sensor names are listed here.

To add a compound rule

1 In GMS mode, go to *Security Console* > *Policy Objects* > *Data Leak Prevention* > *Compound.*

2 In the Content Pane, select *Create New*.

3 Enter the following information:

Name	The compound rule name.
Comments	An optional description of the compound rule.
Protocol	The network protocol to which the compound rule applies. When you select a protocol, select whether to have the compound rule apply to the items listed under this protocol.
Rule	Select the rule to include in the compound rule. For more information about DLP rules, see
Add Rule icon	Select to have another rule selection appear. This way, multiple rules may be added to the compound rule.

4 Select *OK*.

Configuring DLP rules

DLP rules are the core element of the data leak prevention feature. These rules define the data to be protected so the FortiGate unit can recognize it. For example, an included rule uses regular expressions to describe Social Security number:

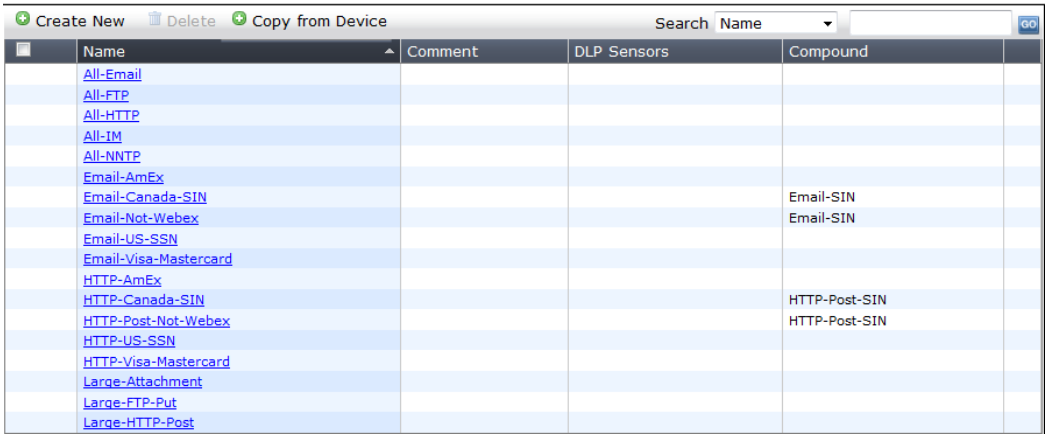
```
([0-6]\d{2}|7([0-6]\d|7[0-2]))[ \-]?\d{2}[ \-]\d{4}
```

Rather than having to list every possible Social Security number, this regular expression describes the structure of a Social Security number. The pattern is easily recognizable by the FortiGate unit.

DLP rules can be combined into compound rules and they can be included in sensors. If rules are specified directly in a sensor, traffic matching any single rule will trigger the configured action. If the rules are first combined into a compound rule and then specified in a sensor, every rule in the compound rule must match the traffic to trigger the configured action.

Individual rules in a sensor are linked with an implicit OR condition while rules within a compound rule are linked with an implicit AND condition.

Figure 120: DLP rule list



Create New	Select to add a rule. For more information, see "To add a DLP rule" on page 181.
Delete	Select the check box beside a rule that you want to delete, then select *Delete* to remove it. You cannot delete a rule that is used by a compound rule or a sensor.
Copy from Device	Select to import a rule configuration from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the compound rule list. Select *Name, Comment, Compound, or DLP Sensors* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of an entry in the list, and right-click to edit it. Select the checkbox of multiple groups in the list to delete, or clone the groups. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name that identifies the rule. Select to view or edit a rule.
Comment	An optional description of each rule.
DLP sensors	If the rule is used in any sensors, the sensor names are listed here.
Compound	If the rule is included in any compound rules, the compound rule names are listed here.

To add a DLP rule

1 In GMS mode, go to *Security Console* > *Policy Objects* > *Data Leak Prevention* > *Rule*.

2 In the Content Pane, select *Create New*.

3 Complete the following:

Name	The name of the rule.
Comments	An optional comment describing the rule.

Protocol	Select the type of content traffic that the DLP rule the rule will apply to. The available rule options vary depending on the protocol that you select. You can select the following protocols: *Email*, *HTTP*, *FTP*, *NNTP*, and *Instant Messaging*.
AIM, ICQ, MSN, Yahoo!	When you select the *Instant Messaging* protocol, you can configure the rule to apply to file transfers using any or all of the supported IM protocols (AIM, ICQ, MSN, and Yahoo!). Only file transfers using the IM protocols are subject to DLP rules. IM messages are not scanned.
HTTP POST, HTTP GET	When you select the *HTTP* protocol, you can configure the rule to apply to HTTP post or HTTP get traffic or both.
FTP PUT, FTP GET	When you select the *FTP* protocol, you can configure the rule to apply to FTP put, or FTP get traffic or both.
SMTP, IMAP, POP3	When you select the *Email* protocol, you can configure the rule to apply to any or all of the supported email protocols (SMTP, IMAP, and POP3).
SMTPS IMAPS POP3S	When you select the *Email* protocol, if your FortiGate unit supports SSL content scanning and inspection, you can also configure the rule to apply to SMTPS, IMAPS, POP3S or any combination of these protocols.
Rule	Use the *Rule* settings to configure the content that the DLP rule matches.
Body	Search for the specified string in the message or page body. This option is available for Email, HTTP, and NNTP.
Subject	Search for the specified string in the message subject. This option is available for Email.
Server	Search for the server's IP address in a specified address range. This option is available for FTP, NNTP.
Sender	Search for the specified string in the message sender user ID or email address. This option is available for Email and IM. For email, the sender is determined by the From: address in the email header. For IM, all members of an IM session are senders and the senders are determined by finding the IM user IDs in the session.
Receiver	Search for the specified string in the message recipient email address. This option is available for Email.
Attachment size	Check the attachment file size. This option is available for Email.
Attachment type	Search email messages for file types or file patterns as specified in the selected file filter. This option is available for Email.
Attachment text	Compare email message files with text found in a RegEx expression.
URL	Search for the specified URL in HTTP traffic.
Transfer size	Check the total size of the information transfer. In the case of email traffic for example, the transfer size includes the message header, body, and any encoded attachment.
Cookie	Search the contents of cookies for the specified text. This option is available for HTTP.
CGI parameters	Search for the specified CGI parameters in any web page with CGI code. This option is available for HTTP.
HTTP header	Search for the specified string in HTTP headers.
Hostname	Search for the specified host name when contacting a HTTP server.
Server	Match a IP to a range of addresses designated for servers.

File type	Search for the specified file patterns and file types. The patterns and types configured in file filter lists and a list is selected in the DLP rule. For more information about file filter lists, see the *FortiGate Administration Guide*. This option is available for FTP, HTTP, IM, and NNTP.
File text	Search for the specified text in transferred text files. This option is available in FTP, IM, and NNTP.
Binary file pattern	Search for the specified binary string in network traffic.
Authenticated User	Search for traffic from the specified authenticated user.
User group	Search for traffic from any user in the specified user group.
File is/not encrypted	Check whether the file is or is not encrypted. Encrypted files are archives and MS Word files protected with passwords. Because they are password protected, the FortiGate unit cannot scan the contents of encrypted files.
Rule operators:	
matches/does not match	This operator specifies whether the FortiGate unit is searching for the presence of specified string, or for the absence of the specified string. • Matches: The rule will be triggered if the specified string is found in network traffic. • Does not match: The rule will be triggered if the specified string is not found in network traffic.
ASCII/UTF-8	Select the encoding used for text files and messages.
Regular Expression/Wildcard	Select the means by which patterns are defined. For more information about wildcards and regular expressions, see the *FortiGate Administration Guide*.
is/is not	This operator specifies if the rule is triggered when a condition is true or not true. • Is: The rule will be triggered if the rule is true. • Is not: The rule will be triggered if the rule is not true. For example, if a rule specifies that a file type is found within a specified file type list, all matching files will trigger the rule. Conversely, if the rule specifies that a file type is not found in a file type list, only the file types not in the list would trigger the rule.
==/>=/<=/!=	These operators allow you to compare the size of a transfer or attached file to an entered value. • == is equal to the entered value. • >= is greater than or equal to the entered value. • <= is less than or equal to the entered value. • != is not equal to the entered value.

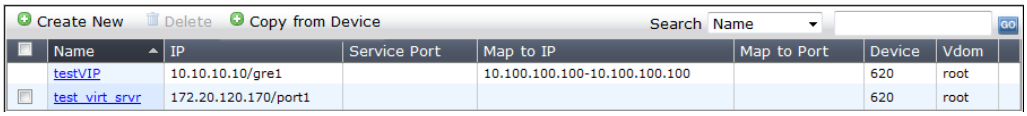
4 Select *OK*.

Configuring virtual IPs

In GMS mode, Virtual IP addresses (VIPs) can be used when configuring firewall policies to translate IP addresses and ports of packets received by a network interface, including a modem interface.

For more information, see the FortiGate documentation.

Figure 121: VIP list



Create New	Select to add a VIP. For more information, see "To add a VIP" on page 184.
Delete	Select the check box beside a VIP that you want to delete, then select *Delete* to remove it. You cannot delete the server if it belongs to a VIP group.
Copy from Device	Select to import a VIP configuration from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the VIP list. Select *Name, IP, Server Port, Map to IP, or Map to Port* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of an entry in the list, and right-click to edit it. Select the checkbox of multiple groups in the list to delete, or clone the groups. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name that identifies the VIP. Select to view or edit a VIP.
IP	The external IP address or IP address and bound network interface, separated by a slash (/).
Service Port	The external port number or port number range. This field is empty if the virtual IP does not specify port forwarding.
Map to IP	The mapped to IP address on the destination network.
Map to Port	The mapped to port number. This field is empty if the virtual IP does not specify port forwarding.
Device	The device on which the VIP is created.
VDOM	The Vdom on which the VIP is created.

To add a VIP

1 In GMS mode, go to *Security Console* > *Policy Objects* > *Virtual IP* > *Virtual IP*.

2 In the Content Pane, select *Create New*.

3 Enter the following information:

Name	Enter the name of the user group.
Device	Select the device for the VIP.
VDOM	If you want to create a VIP for a VDOM, select the VDOM.
External Interface	Select the virtual IP external interface from the list. The external interface is connected to the source network and receives the packets to be forwarded to the destination network.
Type	Select the VIP type: *Static NAT* or *Server Load Balance*. The *Load Balance* type is set in CLI only for the FortiGate units and read-only on the FortiManager system.
External IP Address/Range	Enter the external IP address that you want to map to an address on the destination network. To configure a dynamic virtual IP that accepts connections for any IP address, set the external IP address to 0.0.0.0. For a static NAT dynamic virtual IP you can only add one mapped IP address. For a load balance dynamic virtual IP you can specify a single mapped address or a mapped address range.
Mapped IP Address/Range	Enter the real IP address on the destination network to which the external IP address is mapped. You can also enter an address range to forward packets to multiple IP addresses on the destination network. For a static NAT virtual IP, if you add a mapped IP address range the Fortinet unit calculates the external IP address range and adds the IP address range to the External IP Address/Range field. This option appears only if *Type* is *Static NAT*.
Port Forwarding	Select to perform port address translation (PAT).

Protocol	Select the protocol of the forwarded packets. This option appears only if *Port Forwarding* is enabled.
External Service Port	Enter the external interface port number for which you want to configure port forwarding. This option appears only if *Port Forwarding* is enabled.
Map to Port	Enter the port number on the destination network to which the external port number is mapped. You can also enter a port number range to forward packets to multiple ports on the destination network. For a virtual IP with static NAT, if you add a map to port range the Fortinet unit calculates the external port number range and adds the port number range to the External Service port field. This option appears only if *Static NAT* type is selected and *Port Forwarding* is enabled.

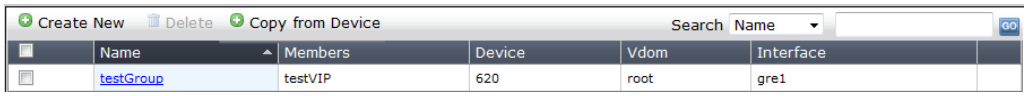
4 Select *OK*.

Configuring virtual IP groups

You can organize multiple virtual IPs into a virtual IP group to simplify your firewall policy list. For example, instead of having five identical policies for five different but related virtual IPs located on the same network interface, you might combine the five virtual IPs into a single virtual IP group, which is used by a single firewall policy.

Firewall policies using VIP groups are matched by comparing both the member VIP IP address(es) and port number(s).

Figure 122: VIP group list



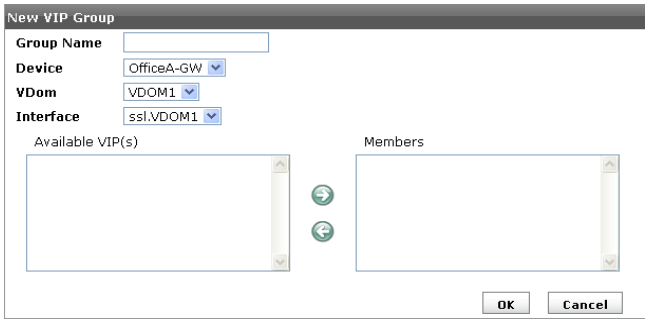
Create New	Select to add a VIP group. For more information, see "To add a VIP group" on page 185.
Delete	Select the check box beside a VIP group that you want to delete, then select *Delete* to remove it. You cannot delete a group that is currently being used by a firewall policy or included in another VIP group.
Copy from Device	Select to import a VIP group configuration from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the VIP group list. Select *Name, Members, or Interface* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of an entry in the list, and right-click to edit it. Select the checkbox of multiple groups in the list to delete, or clone the groups. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The name that identifies the VIP group. Select to view or edit a VIP group.
Members	The VIPs included in the VIP group.
Device	The device on which the VIP group is created.
VDOM	The Vdom on which the VIP group is created.
Interface	The interface for which you want to create the VIP group.

To add a VIP group

1 In GMS mode, go to *Security Console* > *Policy Objects* > *Virtual IP Group*.

2 Select *Create New*.

Figure 123: Creating VIP groups



Group Name	Enter or modify the group name.
Device	Select the device for the VIP group.
VDOM	If you want to create a VIP group for a VDOM, select the VDOM.
Interface	Select the interface for which you want to create the VIP group. If you are editing the group, the Interface box is grayed out.
Available VIPs and Members	Select the right or left arrow to move virtual IPs between *Available VIP(s)* and *Members*. Members contains virtual IPs that are a part of this virtual IP group.

3 Select *OK*.

Configuring global device settings

Policy Objects are related to firewall policies. Device Settings are settings that can apply to system configurations of multiple devices such as DNS, NTP, SNMP, replacement messages, SSL-VPN bookmarks, and FortiGuard settings. Where Policy Objects may be reused multiple times in different policies, Device Settings only have one occurrence.

In GMS mode, the Global Objects window only contains Device Settings. Policy Objects is found in Security Console in GMS mode.

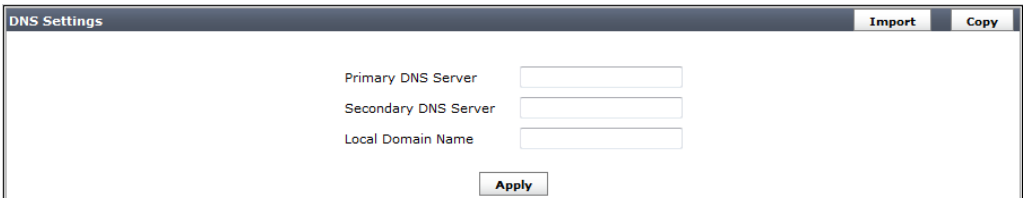
Configure global device settings and copy the configurations to the FortiManager device database for a selected FortiGate unit or a FortiGate group as required.

Configuring DNS

You can specify the IP addresses of the DNS servers to which your devices connect. DNS server IP addresses are usually supplied by your ISP.

To configure DNS servers, go to *Global Objects* > *Device settings* > *DNS*.

Figure 124: Configuring DNS



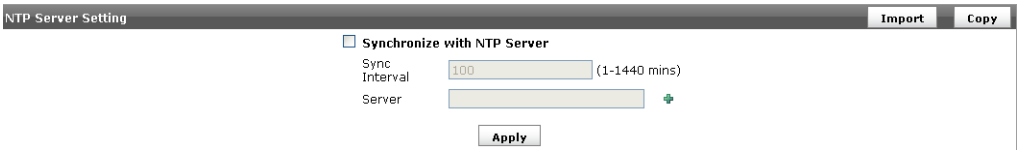
Copy from Device	Select to import a DNS configuration from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Copy	Select to copy the DNS configuration to the selected devices or device groups in the FortiManager device database. For more information, see "To copy a global object" on page 127.
Primary DNS Server	Enter the primary DNS server IP address.
Secondary DNS Server	Enter the secondary DNS server IP address.
Local Domain Name	Enter the domain name to append to addresses with no domain portion when performing DNS lookups.
Apply	Select to save the configuration.

Configuring NTP

You can configure an NTP server to automatically set a device's system date and time. You must specify the server and synchronization interval.

To configure NTP servers, go to *Global Objects* > *Device settings* > *NTP*.

Figure 125: Configuring NTP



Import	Select to import a NTP configuration from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Copy	Select to copy the NTP configuration to the selected devices or device groups in the FortiManager device database. For more information, see "To copy a global object" on page 127.
Synchronize with NTP Server	Select to use an NTP server to automatically set the system date and time. You must specify the server and synchronization interval.
Sync Interval	Specify how often the device should synchronize its time with the NTP server. For example, a setting of 1440 minutes causes the device to synchronize its time once a day.
Server	Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, see http://www.ntp.org. To add more servers, select the + icon.
Apply	Select to save the configuration.

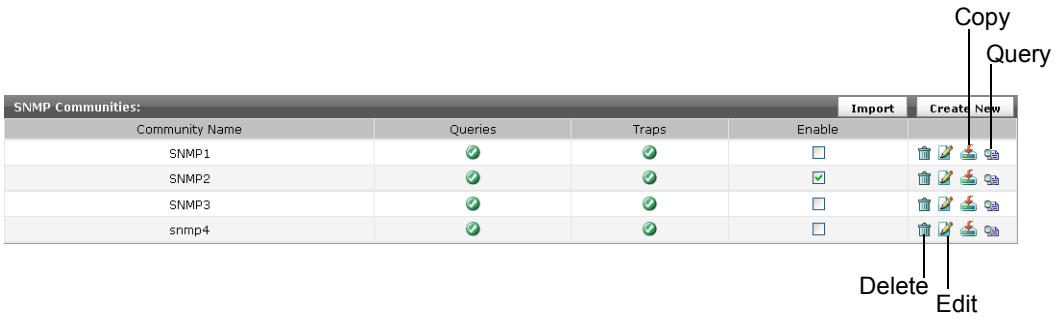
Configuring SNMP

Simple Network Management Protocol (SNMP) allows you to monitor hardware on your network. You can configure the hardware, or SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers. An SNMP manager is a computer running an application that can read the incoming traps from the agent and track the information. The FortiManager system acts as a manager for its managed Fortinet devices.

Using an SNMP manager and Fortinet MIB files, you can access SNMP traps and data from any FortiGate interface or VLAN subinterface configured for SNMP management access. You can download the Fortinet MIB files for your Fortinet devices from the Fortinet support website.

To view the SNMP community list, go to *Global Objects* > *Device settings* > *SNMP*.

Figure 126: SNMP



Import	Select to import an SNMP configuration from the selected device in the FortiManager device database. For more information, see "To import a global object" on page 125.
Create New	Select to add a new SNMP community. For more information, see "Configuring an SNMP community" on page 188.
Community Name	The name of the SNMP community.
Queries	The status of SNMP queries for each SNMP community. The query status can be enabled or disabled.
Traps	The status of SNMP traps for each SNMP community. The trap status can be enabled or disabled.
Enable	Display if the SNMP community is activated.
Delete icon	Select to remove an SNMP community.
Edit icon	Select to view or modify an SNMP community.
Copy	Select to copy the NTP configuration to the selected devices or device groups in the FortiManager device database. For more information, see "To copy a global object" on page 127.
Query icon	Select to view if the SNMP configuration has been saved to the selected devices or device groups in the FortiManager device database. For more information, see "To query device database(s) for a global object" on page 128.

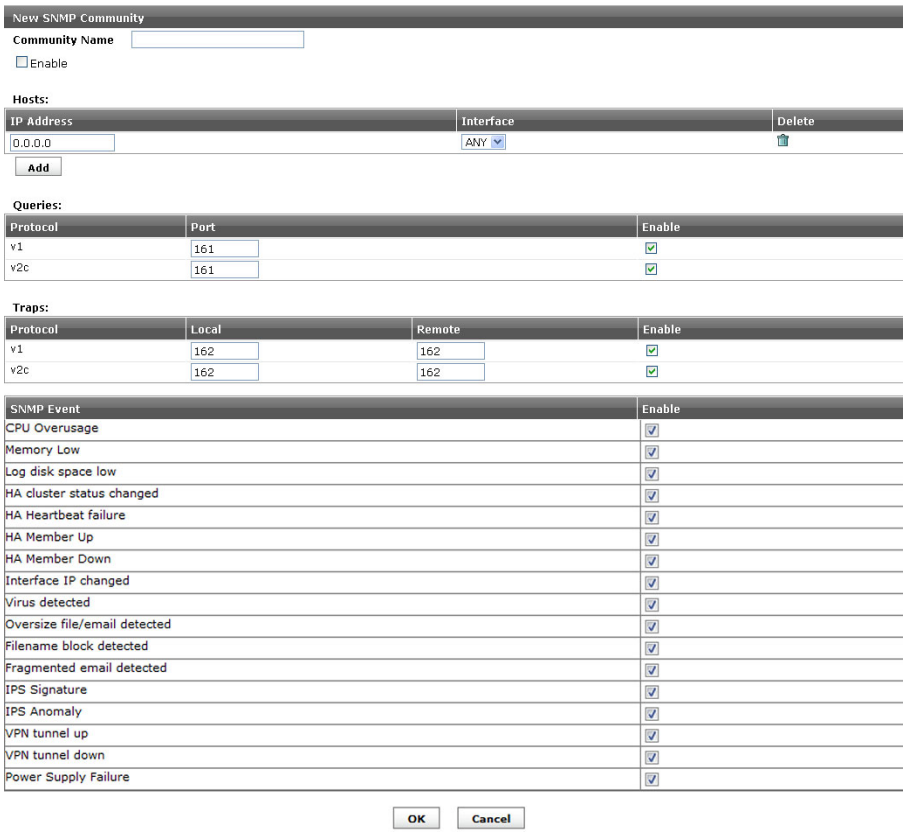
Configuring an SNMP community

An SNMP community is a grouping of equipment for network administration purposes. Add SNMP communities to your device so that SNMP managers can connect to view system information and receive SNMP traps.

Each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the device for a different set of events. You can also add the IP addresses of up to 8 SNMP managers to each community.

SNMP settings in this global object category are for FortiGate units. The FortiGate units are the SNMP agents, and the FortiManager system is managing them. To change SNMP settings for the FortiManager system's SNMP agent, see "SNMP" on page 51.

Figure 127: Configuring SNMP communities



Community Name	Enter a name to identify the SNMP community.
Enable	Select to activate the SNMP community.
Hosts	
IP Address	Enter the IP address of an SNMP manager that can use the settings in this SNMP community to monitor the SNMP agent. You can also set the IP address to 0.0.0.0 to so that any SNMP manager can use this SNMP community.
Interface	Optionally select the name of the interface that this SNMP manager uses to connect to the SNMP agent. You only have to select the interface if the SNMP manager is not on the same subnet as the SNMP agent. This can occur if the SNMP manager is on the Internet or behind a router. In virtual domain mode, the interface must belong to the management VDOM to be able to pass SNMP traps.
Delete	Select to remove an SNMP manager.
Add	Add a blank line to the *Hosts* list. You can add up to 8 SNMP managers to a single community.
Queries	Enter the Port number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the SNMP agent. Select the *Enable* check box to activate queries for each SNMP version.
Traps	Enter the *Local* and *Remote* port numbers (port 162 for each by default) that the SNMP agent uses to send SNMP v1 and SNMP v2c traps to the SNMP managers in this community. Select the *Enable* check box to activate traps for each SNMP version.
SNMP Event	Enable each SNMP event for which the SNMP agent should send traps to the SNMP managers in this community.

Configuring replacement messages

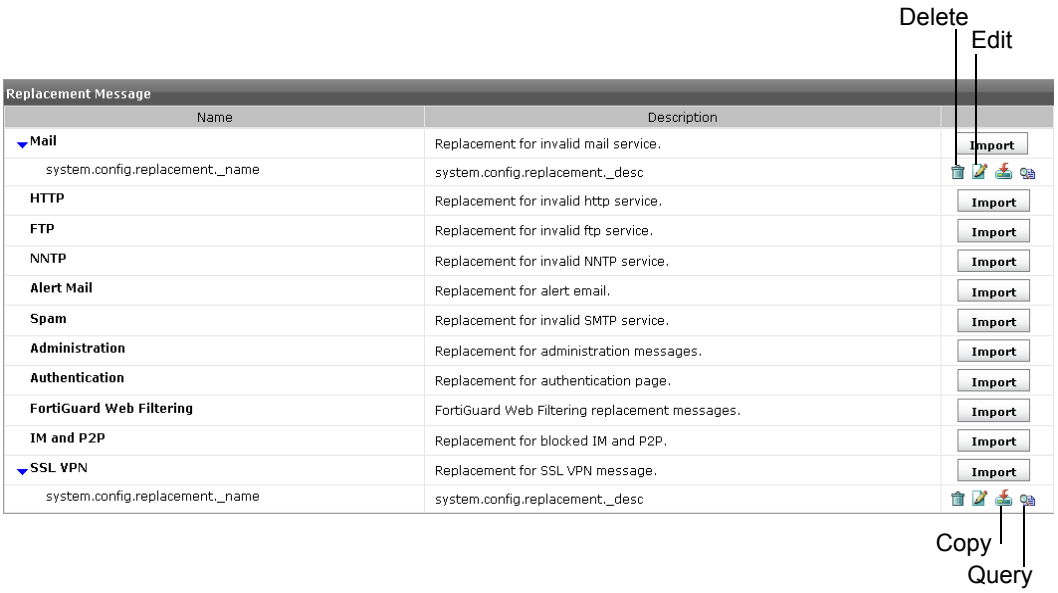
Change replacement messages and customize alert email and information that a FortiGate unit adds to content streams such as email messages, web pages, and FTP sessions.

The FortiGate unit adds replacement messages to a variety of content streams. For example, if a virus is found in an email message, the file is removed from the email and replaced with a replacement message. The same applies to pages blocked by web filtering and email blocked by spam filtering.

Note: Disclaimer replacement messages provided by Fortinet are examples only.

To view the replacement messages list, go to *Global Objects* > *Device settings* > *Replacement Messages*. The list organizes replacement message into an number of types (for example, Mail, HTTP, and so on). After importing a replacement message from a device configuration saved in the FortiManager device database, you can modify the message.

Figure 128: Replacement message list



Name	The type of replacement message. Select the blue triangle to expand or collapse the category. The blue triangle appears after you import a replacement message from a device configuration saved in the FortiManager device database.
Description	Information about which message is replaced.
Import	Select to import a replacement message from a device configuration saved in the FortiManager device database. For more information, see "To import a global object" on page 125.
Delete icon	Select to remove a replacement message.

Edit icon	Select to view or modify a replacement message. You can change the content of the replacement message by editing the text and HTML codes and by working with replacement message tags. For more information about replacement message tags, see the *FortiGate Administration Guide*. For more information about editing a replacement message, see "To edit a replacement message" on page 191.
Copy icon	Select to copy the replacement message configuration to the selected devices or device groups in the FortiManager device database. For more information, see "To copy a global object" on page 127.
Query icon	Select to view if the replacement message has been saved to the selected devices or device groups in the FortiManager device database. For more information, see "To query device database(s) for a global object" on page 128.

To edit a replacement message

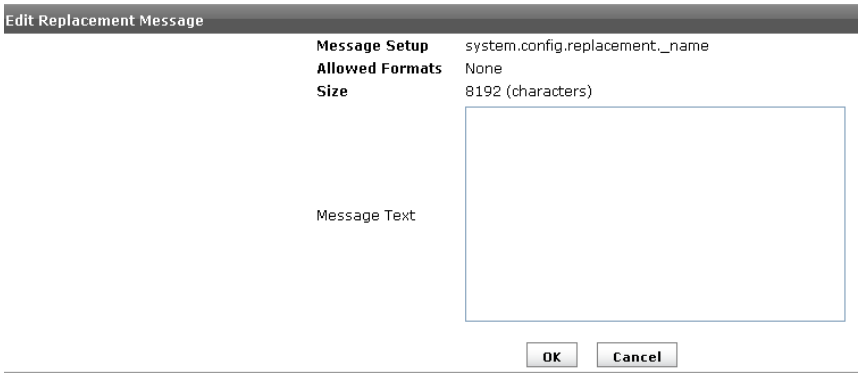
1 Go to *Global Objects* > *Device settings* > *Replacement Messages*.

2 Select an expand arrow (blue triangle) to view the replacement message that you want to change.

The expand arrow only appears after you import a replacement message from a device configuration saved in the FortiManager device database.

3 Select the *Edit* icon for the message that you want to edit.

Figure 129: Editing a replacement message



4 Complete the following:

Message Setup	The name of the replacement message.
Allowed Formats	The type of content that can be included in the replacement message. Allowed formats can be Text or HTML. You should not use HTML code in Text messages. You can include replacement message tags in text and HTML messages.
Size	The size limit for the test message.
Message Text	The editable text of the replacement message. The message text can include text, HTML codes (if HTML is the allowed format) and replacement message tags.

5 Select *Ok*.

Configuring SSL VPN bookmarks

If you create a user account that permits web-only mode access, you can create hyperlinks to frequently accessed server applications that the user can select to start a session from his or her home page.

The FortiGate unit forwards client requests to servers on the Internet or internal network. To use the web-portal applications, you add the URL, IP address, or name of the server application to the bookmarks list. The bookmarks are available when the user starts an active SSL VPN session.

To view the list of existing SSL VPN bookmarks, go to *Global Objects* > *Device settings* > *SSL-VPN* > *Bookmarks.* The list details the name of the bookmark, type of bookmark, and the link details.

Figure 130: Bookmark list

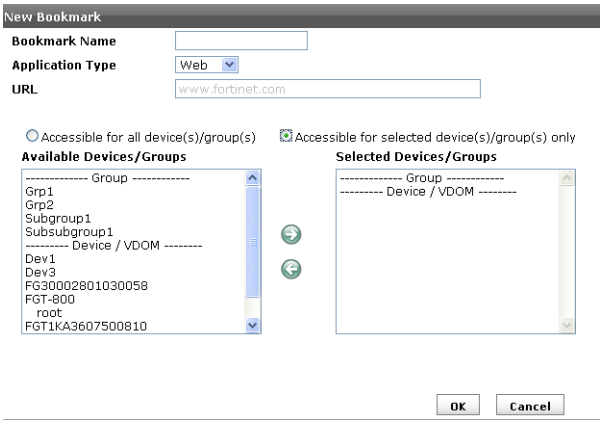
Create New	Select to add a bookmark. For more information, see "To add a SSL VPN bookmark" on page 192.
Delete	Select the check box beside a SSL VPN bookmark that you want to delete, then select *Delete* to remove it. You cannot delete a bookmark that is included in a bookmark group.
Copy from Device	Select to import a bookmark from a device configuration saved in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the SSL VPN bookmark list. Select *Bookmark Name, Application Type, or Link* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of a bookmark in the list, and right-click to delete, edit, clone or select all. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The types and names of links to remote server applications and network services.
Application Type	The abbreviated name of the server application or network service. For more information, see "To add a SSL VPN bookmark" on page 192.
Link	The URL, host, or folder of the bookmark link.
Filter	Display if the SSL VPN bookmark configuration is used at the individual devices or groups level. If specific devices and/or groups are listed, it means that they are not using the configuration. If *All Devices/Groups* displays, it means that the configuration is used on all devices and groups. If *No Devices/Groups* appears, it means that the *Limit Visibility from Device Level* option is selected but no devices or device groups are selected for not using the configuration. For more information, see "To add a SSL VPN bookmark" on page 192.

To add a SSL VPN bookmark

1 Go to *Global Objects* > *Device settings* > *SSL-VPN* > *Bookmarks.*

2 Select *Create New.*

Figure 131: Adding SSL VPN bookmarks



3 Complete the following:

Bookmark Name	Enter the name for the bookmark.
Application Type	Select the abbreviated name of the server application or network service from the drop-down list: • Web • Telnet • FTP • SMB • VNC • RDP • SSH
URL/Host/Folder	Type the information that the FortiGate unit needs to forward client requests to the correct server application or network service: • If the application type is Web, type the URL of the web server (for example, www.example.com). • If the application type is Telnet, type the IP address of the telnet host (for example, 10.10.10.10). • If the application type is FTP, type the IP address of the FTP host as a root directory/folder (for example, //server/folder/). • If the application type is SMB/CIFS, type the IP address of the SMB host and the root directory/folder associated with your account (for example, //server/folder/). • If the application type is VNC, type the IP address of the VNC host (for example, 10.10.10.10). • If the application type is RDP, type the IP address of the RDP host (for example, 10.10.10.10). • If the application type is SSH, type the IP address of the SSH host (for example, 10.10.10.10).
Accessible for all device(s)/group(s)	Select to allow all devices or groups to use the global SSL VPN bookmark configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	Select to allow selected devices or groups to use the global SSL VPN bookmark configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow.

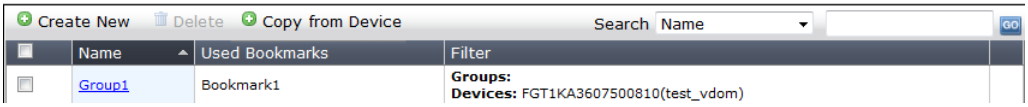
4 Select *Ok*.

Configuring SSL VPN bookmark groups

You can create a group of specific bookmarks to include in the configuration of an SSL VPN bookmark group.

To view the list of existing SSL VPN bookmark groups, go to *Global Objects* > *Device settings* > *SSL-VPN* > *Bookmark Groups.*

Figure 132: Bookmark group list



Create New	Select to add a bookmark group. For more information, see "To add a SSL VPN bookmark group" on page 194.
Delete	Select the check box beside a SSL VPN bookmark group that you want to delete, then select *Delete* to remove it.
Copy from Device	Select to import a bookmark group from a device configuration saved in the FortiManager device database. For more information, see "To import a global object" on page 125.
Search	Search the SSL VPN bookmark group list. Select *Group Name or Bookmarks* and enter the value to search, then select *Go*.
Checkbox	Select the checkbox of an entry in the list, and right-click to edit it. Select the checkbok of multiple groups in the list to delete, or clone the groups. For more on the right-click menu, see "Right-click menu" on page 126.
Name	The names of bookmark groups.
Used Bookmarks	List of bookmarks that are included in the bookmark groups.
Filter	Display the devices and groups that can use the global SSL VPN bookmark group configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration. For more information, see "To add a SSL VPN bookmark group" on page 194.

To add a SSL VPN bookmark group

1. Go to *Global Objects* > *Device settings* > *SSL-VPN* > *Bookmark Groups.*
2. In the Content Pane, select *Create New*.
3. Enter the following information:

Name	Enter a descriptive name for this bookmark group.
Available Bookmarks	The list of bookmarks available for inclusion in the bookmark group. Bookmarks are listed under the appropriate categories — FTP, RDP, SMB, Telnet, VNC, Web, or SSH. Use the right and right arrows to move selected bookmarks to or from the *Used Bookmarks* field.
Used Bookmarks	The list of bookmarks that belong to the bookmark group. Use the left-pointing arrow to move a selected bookmark to the *Available Bookmarks* field.

Accessible for all device(s)/group(s)	Select to allow all devices or groups to use the global SSL VPN bookmark group configuration. This option is selected by default.
Accessible for selected device(s)/group(s) only	Select to allow selected devices or groups to use the global SSL VPN bookmark group configuration. In the *Available Devices/Groups* list, select the devices or groups and move them to the *Selected Devices/Groups* list by using the right-pointing arrow. See "Accessibility options - EMS mode" on page 129.

4 Select *Ok*.

Configuring FortiGuard settings

Worldwide coverage of FortiGuard services is provided by FortiGuard service points. When the Fortinet unit is connecting to the FortiGuard Distribution Network (FDN), it is connecting to the closest FortiGuard service point in the world. Fortinet adds new service points as required.

You can choose an override server if you cannot connect to the FDN or if your organization provides updates using their own FortiGuard server.

For additional FortiGuard settings, including delaying updates, see "FortiGuard Center" on page 79. For more information about the FortiGuard services, see the *FortiGate Administration Guide*.

To configure FortiGuard settings

1 Go to *Global Objects* > *Device settings* > *FortiGuard*.

2 Complete the following:

Copy	Select to copy the FortiGuard settings to the selected devices or device groups in the FortiManager device database. For more information, see "To copy a global object" on page 127.
Use override server address for FortiGuard AV/IPS Service	Select to configure an override server if you cannot connect to the FDN or if your organization provides AV/IPS service updates using their own FortiGuard server. When selected, enter the IP address or domain name of a FortiGuard server and select *Apply*.
Use override server address for FortiGuard Web Filtering and AntiSpam Service	Select to configure an override server if you cannot connect to the FDN or if your organization provides web filtering and antispam service updates using their own FortiGuard server. When selected, enter the IP address or domain name of a FortiGuard server and select *Apply*.

Security Console

The Security Console enables administrators to configure security elements common to multiple FortiGate units in a central location. Once configured, administrators can push these elements the managed FortiGate units.

The Security Console is only available when running the FortiManager unit in Global Management System (GMS) mode.

The Security Console's centralized configuration makes it easy to view and manage firewall policies, VPN configurations and dynamic objects for many managed devices. Once all configurations are set, you can push the updates in one of three ways, depending on the needs of the managed devices:

- Install a set of common policies that are installed to all devices, that is, the same policy table appears for all devices
- Install a set of policies that map to unique policies on each device, that is, the same type of policies exist, but some properties are unique for each or a few devices
- Install unique policies that can be installed to individual devices or groups, such as Virtual IP policies or site-specific configurations.

The Security Console also includes a revision history. This enables you to view, compare and revert to previous installed configurations. This is very useful should an update to a device fail, due to a configuration error. You can simply revert to the previous version before the changes, and review the configuration to fix any problems.

The following topics are included in this section:

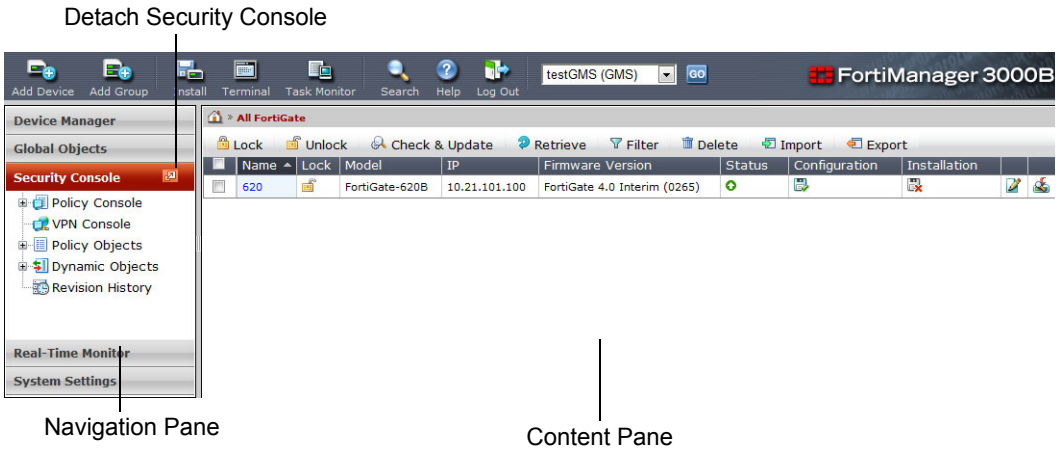
Security Console window

The Security Console window provides an easy-to-view tree of objects. The window enables you to add and edit firewall policies, protection profile options and port addressing, and more which can then be pushed to FortiGate units.

There are three parts:

- the list of object categories in the Navigation Pane
- the configuration and setting information in the Content Pane
- the Detach Security Console button to make the Security Console Window into a separate window from the rest of the FortiManager system display.

Figure 133: Security Console window



Detach Security Console

An icon at the top of the Security Console window enables you to detach the Security Console from the Navigation Pane. The new window includes a new Main Menu Bar at the top, the Security Console window is in the Navigation Pane location, and Content is displayed in the Content Pane of this detached window.

The detached Security Console's Main Menu Bar includes buttons for Install, Task Manager, Save, Search, Help, and Close. It does not include the Device Manager buttons, or the System buttons found in the main FortiManager system display.

The Detached Security Console Main Menu Bar has two unique buttons — Save and Close.

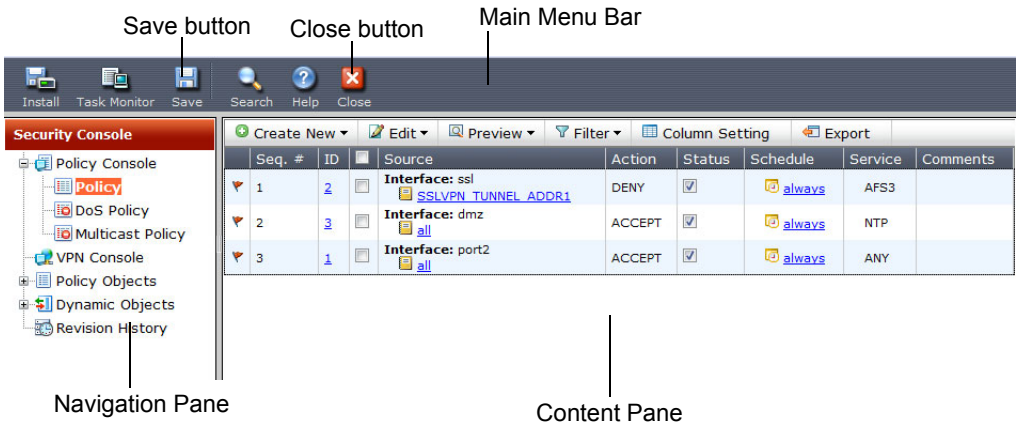
Save button

Selecting the save button takes you to the revision history page where you can save the current revision, or restore to a previous version. See "Revision History" on page 207.

Close button

Selecting the close button closes the detached Security Console. All Security Console information returns to the Navigation Pane where you can continue working with it as before.

Figure 134: Detached Security Console



Navigation Pane

The Navigation Pane contains the following major nodes. The Content Pane content depends on the node selected in the Navigation Pane.

Policy Console	You can create regular and VPN firewall policies to copy to your devices. Use dynamic objects to ensure that device-specific settings are correctly applied. For more information, see "Dynamic Objects" on page 206.
VPN Console	You can create a VPN by specifying the topology type, the IKE settings, and the gateway devices. For more information, see "Policy Console" on page 199.
Policy Objects	You can create objects to be used in firewall policies. Policy objects are parts of a firewall configuration such as addresses, pre-defined service groups, and protection profiles. Once configured, these objects can be easily combined into any number of firewall policies using the Policy Console. For more information, see "Configuring global policy objects" on page 128.
Dynamic Objects	A configuration object whose value differs from one device to another can be mapped to the appropriate setting for each device. You can then use this dynamic object in a policy that you copy to multiple devices. There are dynamic objects for interfaces, addresses and NAT settings. For more information, see "Dynamic Objects" on page 206.
Revision History	The Revision History enables you to view, compare and revert to previous installed configurations. Should something unwanted occur with a new configuration install, the Revision History enables you to roll back to an configuration that has proven to work. For more information, see "Revision History" on page 207.

Policy Console

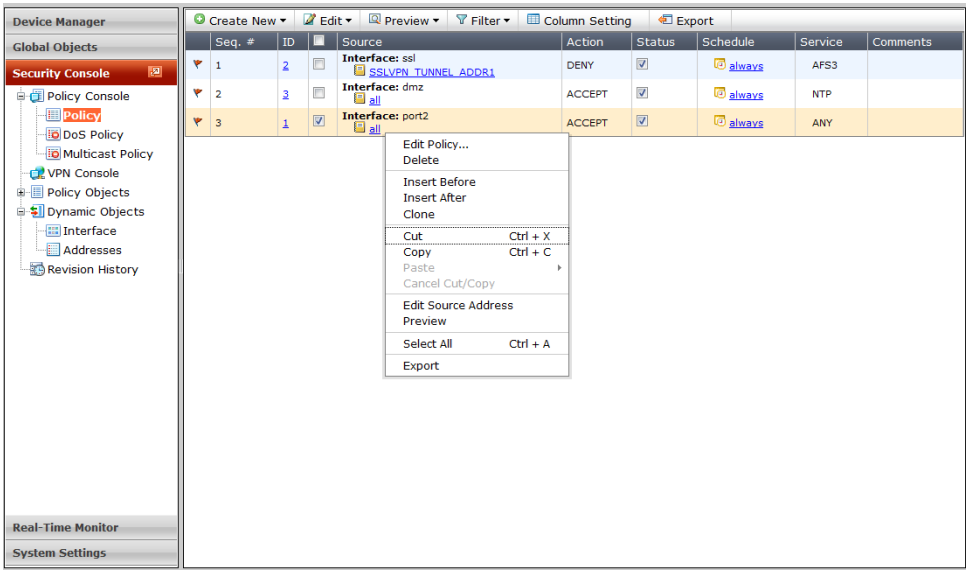
Use the Policy Console to create regular, VPN and DoS firewall policies, and install them.

Select one or more policies using the checkboxes, and right-click for a menu of available actions. The available actions varies with the objects being configured, and if multiple objects were selected. The right-click menu actions allow for easy manipulation of large numbers of objects.

Left click to select a policy, hold down on the button, and drag the policy to the place in the list where you want to move it to. Release the mouse button to drop the policy in place. While you are moving the policy it will be outlined, and the position it will be inserted into is highlighted.

Use Export to send your policies to your management computer in CSV format. This is very useful for company security policy audits, and the CSV format is compatible with many common spreadsheets, databases, and other applications.

Figure 135: Policy Console window



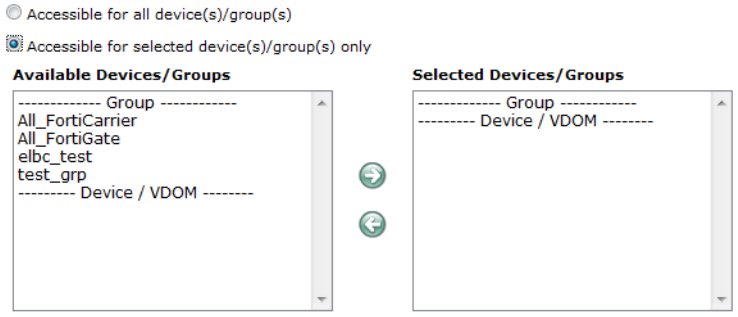
Flag	A red flag indicates this policy has not been installed on a device. Select the policy and then select Install. See "Installing Device Configurations" on page 277.
Seq. #	The sequence number of the policies. If you reorder the policies, the sequence numbers remain in the same order, and the ID numbers move with the policies.
ID	The ID number of the policy. This is a unique number assigned to the policy. If you reorder the policies, this number moves with the policy no matter what the new order is. When moving a policy, policy IDs are used to indicate the new location.
Create New	Create a new policy. Select from a regular or VPN firewall policy. The default policy type is regular firewall policy. Use the drop-down list on the right side of the button to select other options. See "Creating regular and VPN firewall policies" on page 201. You can also create a a section title in the policy list. Enter a name for the section and the policy ID where the section begins, then select *Apply*.
Edit	Select to edit, delete, or move the selected policy or policies. Some or all of these options will not be available depending on how many policies are selected. If no policies are selected, no options are available. If one policy is selected, all options are available. If multiple policies are selected, only delete is available.
Preview	Select to preview selected policies by device or by policy. The preview shows the basics of the policy — devices, source and destination ports and addresses, NAT, IP Pool, Fixed port To preview by policy, you must select only one policy.
Filter	Select to set or clear display filter. The filter specifies which policies are displayed by setting conditions for one or more columns. You can also clear existing filters. See "To set policy filters" on page 201.
Column Setting	Choose the columns to display in the table. You can also determine the order in which columns display.
Export	Select to export the selected policy or policies in comma separated value (CSV) format to your computer. CSV format is compatible with spreadsheets, databases, and many other applications.

Accessibility options

Policy Console objects that you configure include accessibility options at the bottom of the window. These options indicate if the global object is to be available to all devices or only to small set of devices or groups.

When you select the option *Accessible for selected device(s)/group(s) only*, the available and selected devices/groups lists appear and you can transfer groups and devices from one list to the other.

Figure 136: Accessibility options



Filtering policies

If you are managing multiple FortiGate units, you can potentially have hundreds of firewall policies to control and monitor network traffic through the firewall. The *Filter* button on the Policy Console enables you to locate policies that you need, without having to comb through policies. When you select the Filter button, you can select the filter criteria, that is the column of information, and its contents. For example, you can filter on service, and select to view only those policies that contain HTTPS services (allow or deny) in the policy.

To set policy filters

1. On the *Policy* page, select the *Filter* button.

   The *Policy Filter* window opens.
2. If you want to remove existing filters, select *Clear all Filters*.
3. In the list on the left, select the column that you want to filter.
4. On the right, select *Enable*.
5. Set the filtering criteria. These depend the column that you selected.
6. Repeat steps 3 through 5 for each column that you want to filter.

   Policies that meet the criteria for all filtered columns will be displayed in the policy list.
7. Select *OK*.

Creating regular and VPN firewall policies

Regular firewall policies govern traffic between device interfaces based on source and destination addresses, type of service and schedules. Optionally, a policy can apply a protection profile, require authentication or endpoint compliance checks. For more information about firewall policies, see the Firewall Policy chapter of the *FortiGate Administration Guide*.

To create a regular firewall policy

1 Go to *Security Console* > *Policy Console* > *Policy*.

2 Select *Create New* > *Policy*.

3 Configure the remaining settings as you would for a FortiGate unit firewall policy.

For some policy settings, you can select policy objects and dynamic objects that you have created. For services, interfaces, and protection profiles, there are also some predefined values.

To use dynamic NAT objects, select *NAT* and *Dynamic NAT* and then select the Dynamic NAT object from the list. For more information, see "Dynamic Objects" on page 206.

4 If the policy does not apply to all devices, select *Accessible for selected device(s)/group(s) only*. Make selections in the *Available Devices/Groups* list and then select the right-arrow button to move them to the *Selected Devices/Groups* list. See "Accessibility options" on page 201.

5 Select *OK*.

To create a VPN firewall policy

1 Go to *Security Console* > *VPN Console*, and create a VPN configuration. See "VPN Console" on page 203.

2 Go to *Security Console* > *Policy Console* > *Policy*.

3 Select *Create New* > *VPN Policy*.

4 From the *VPN* list, select the VPN configuration you created in the VPN Console.

5 If the policy applies to all devices where it is relevant, select *Apply to Traffic between All Protected Subnets*. Otherwise, select *Specify Source/Destination Protected Subnets* and then specify the devices and protected subnet addresses for *Source(s)* and *Destination(s)*. See "Accessibility options" on page 201.

6 Configure the remaining settings as you would for a FortiGate unit VPN firewall policy.

For the *Schedule*, you can select a schedule policy object that you have already created in *Policy Objects*. See "Configuring firewall schedules" on page 135.

Creating DoS policies

Denial of Service (DoS) policies are primarily used to apply DoS sensors to network traffic by FortiGate interface. DoS sensors identify anomalous network traffic that does not fit known or common traffic patterns and behavior.

To create a DoS Policy

1 Go to *Security Console* > *Policy Console* > *DoS Policy*.

2 Select *Create New* > *Policy*.

3 Select the Source *Interface/Zone* and *Address Name*.

4 Select the Destination *Address Name* and *Service*.

5 Select the *DoS Sensor* check box and then select a *DoS Sensor* from the list.

To create DoS Sensors, go to *Policy Objects* > *IPS Sensor* > *IPS DoS Sensor* in the *Security Console*. For more information, see "Configuring IPS DoS sensors" on page 143.

6 Select *OK*.

Creating Multicast policies

Multicast destination NAT (DNAT) allows you translate externally received multicast destination addresses to addresses that conform to an organization's internal addressing policy.

By using this feature, you can avoid redistributing routes at the translation boundary into their network infrastructure for Reverse Path Forwarding (RPF) to work properly. They can also receive identical feeds from two ingress points in the network and route them independently.

FortiGate units offer multicast policies only through the CLI.

To create a multicast Policy

1. Go to *Security Console* > *Policy Console* > *Multicast Policy*.
2. Select *Create New* > *Policy*.
3. Enter the Source *Interface*, *Address*, and *NAT* address.
4. Enter the Destination Interface, *Address, and Nat.*
5. Enter the *Protocol, Start Port*, and *End Port*.
6. Select an *Action* of ACCEPT or DENY for this policy.
7. If the policy applies to all devices where it is relevant, select *Apply to Traffic between All Protected Subnets*. Otherwise, select *Specify Source/Destination Protected Subnets* and then specify the devices and protected subnet addresses for *Source(s)* and *Destination(s)*. See “Accessibility options” on page 201.
8. Select *OK*.

Installing firewall policies

Firewall policies in the Security Console are pushed down to the FortiGate units as a batch install of all the policies, to all the managed FortiGate units.

The devices must be locked before any changes are pushed to them. See “Device configuration locks” on page 69, and “Device Manager window” on page 81.

To send the firewall policy to the FortiGate units, select *Install*. You can select to install to a complete security domain, FortiGate units, or FortiCarrier units. For more information on installing configurations to devices, see “Installing Device Configurations” on page 277.

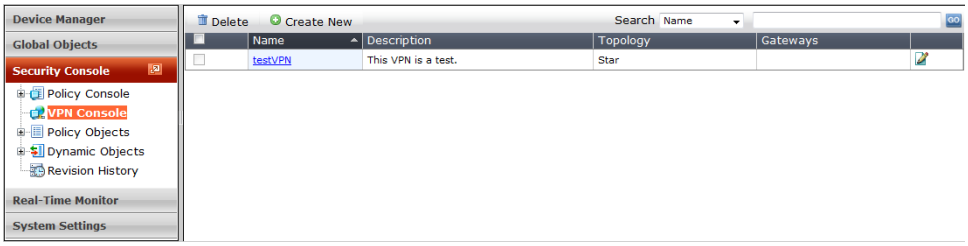
VPN Console

The VPN Console enables you to create VPN configurations and copy them to the managed FortiGate units. To see the list of VPN configurations, go to *Security Console* > *VPN Console*.

When you have a VPN Console in the Content Pane list, selecting the name of that entry will take you to a new screen. From there you can create gateways and subnets for that VPN console. These are required if you configure a VPN Policy and select *Specify Source/Destination Protected Subnets* for the *Policy Scope*. See “Creating regular and VPN firewall policies” on page 201.

There is no right-click menu available for the VPN Console list.

Figure 137: VPN List



Delete	To delete a VPN configuration, select one or more configurations from the list by selecting its check box, then select *Delete*.
Create New	Create a new VPN configuration.
Search	To locate a VPN configuration, select a search criteria from the drop down list box, enter the keyword text in the text box beside and select ***Go***.
Checkbox	Select one or more VPN Console entries to delete.
Name	The VPN name.
Description	Optional description.
Topology	One of: **Full Meshed** — each gateway has a tunnel to every other gateway **Star** — each gateway has one tunnel to a central hub gateway **Dialup** — some gateways, often mobile users, have dynamic IP addresses and contact the gateway to establish a tunnel
Gateways	The FortiGate units that function as the VPN tunnel ends.
Edit icon	Edit this VPN configuration.

Configuring a VPN

To create a VPN, you need to:

- Create firewall addresses for your VPN's protected subnets.
- Create the VPN configuration.
- Add VPN gateways.
- Create VPN firewall policies in the Policy Console.

Create a firewall address

Ensure the port needed to begin or end the VPN tunnel is setup with a valid IP address and netmask. These addresses will be used by the firewall policy for the source and destination addresses of the VPN policy.

To create a firewall address

1 Go to *Security Console* > *Policy Objects* > *Address* > *Address*.

2 Select *Create New*.

3 Enter the port address information and select *OK*.

Create a VPN configuration

The VPN configuration defines the structure of the VPN tunnel. It includes the type of tunnel to create, and the encryption/security level to apply to the tunnel. The configuration you create in the steps below are applied in the VPN firewall policy.

To create a VPN configuration

1. Go to *Security Console* > *VPN Console*.
2. Select *Create New*.
3. Enter a name for the VPN.
4. Select the VPN *Topology* to use.
5. Enter the *IKE Phase 1* and *IKE Phase 2* settings.
6. For *Pre-shared Key*, select *Generate (random)* or select *Specify* and enter the key.
7. Select *OK*.

Add a VPN gateway

Create a VPN gateway. This is the address/port combination the VPN tunnel will use to route traffic.

Note: You must set one or more Protected Subnets for the VPN Console to be able to select *Specify Source/Destination Protected Subnet* under the *Policy Scope*. If you do not, the list will be empty and you will have to select *Apply to Traffic between All Protected Subnets* instead. See "Creating regular and VPN firewall policies" on page 201.

To add a VPN gateway

1. Go to *Security Console* > *VPN Console*.
2. In the Content Pane VPN list, select the name of a VPN Console entry.
3. Select *Create New*.
4. Select the *Device* for the VPN gateway. This device must already exist in the FortiManager database. To add new devices, see "Adding a device" on page 84.
5. Select the *Default VPN Interface* on the VPN device that connects the VPN to the public network.
6. Select the *Node Type* as one of HUB or Spoke.
7. Select the routing options. Select *Manual* to create the route yourself in Device manager or select *Automatic* for the VPN console to automatically configure the interface on the VPN device that connects the VPN to the public network.
8. Select the *Protected Subnet* by selecting the configured interface and firewall address for that network and then select the plus ("+") icon to apply the entry. Repeat for each protected subnet.
9. Select *OK*.

Create VPN firewall policies

Create the firewall policies that allows the network traffic through the FortiGate units completing the tunnel.

To create VPN firewall policies

1. Go to *Security Console* > *Policy Console* > *Policy.*
2. Select *Create New* > *VPN Policy.*
3. Select the VPN object connected to the firewall policy.

4 Select a *Policy Scope*.

If you select *Specify Source/Destination Protected Subnets*, you must select the source and destination device and subnets from the VPN gateway *Protected Subnets* configured in "Add a VPN gateway" on page 205.

5 Select *Always* for the *Schedule*.

6 Select *Any* for the *Service*.

7 Select *Accept* for the *Action*.

8 Configure the remaining fields as required.

9 Select *OK*.

For information on installing the firewall policies on the FortiGate units, see "Installing firewall policies" on page 203.

Dynamic Objects

Interfaces, firewall addresses, and dynamic NAT configurations vary from one device to another. You can configure these objects in the Security Console as dynamic objects and map them to individual devices. Dynamic Objects are available in GMS mode only, within the Security Console. You can select the dynamic objects when you create policies in the Policy Console.

In EMS mode, dynamic objects are not available. You must configure FortiGate devices individually. For convenience, you can create common objects, such as protection profiles, in the Configuration Database and use them in device configurations.

Dynamic Objects windows do not support right-click menus. Create New buttons are located on the right side of the Content Pane.

Predefined Interface

Predefined Interface displays a list of all the factory default interfaces on FortiGate models. This list is useful as a reminder if you are creating objects and managing remote devices. For each interface its name, real name, and models it appears on are listed. This list cannot be changed.

To view a list of predefined device interfaces, go to *Security Console* > *Dynamic Objects* > *Interface* and expand *Predefined Interface*.

Creating dynamic objects

All of the dynamic object types are created using a similar method. You create a default mapping for the object and then specify the mappings for devices that require a different mapping.

To configure a dynamic interface object

1 Go to *Security Console* > *Dynamic Objects* > *Interface* and select *Create New*.

2 Enter a *Name* for the interface object.

3 Optionally, enter a descriptive *Comment*.

4 If most of the devices have the same name for this interface, enter this name as the *Default Mapping*.

5 In the *Mapping Rules* section, select a *Device* that does not use the default mapping, select the *Interface* mapping for that device, and then select the plus ("+") icon.

6 Repeat step 5 for each device that does not use the default mapping.

Use the up and down arrows for an entry to adjust its position in the list. Use the delete icon to remove a mapping rule from the list.

7 Select *OK*.

Note: You must create the firewall address policy objects that you need before you create dynamic address objects. For more information, see "Configuring firewall addresses" on page 132.

To configure a dynamic address object

1 Go to *Security Console* > *Dynamic Objects* > *Addresses* and select *Create New*.

2 Enter a *Name* for the dynamic address object.

3 Optionally, enter a descriptive *Comment*.

4 Select the default address in *Default Mapping*.

5 In the *Mapping Rules* section, select a *Device* that does not use the default mapping, select the *Address* settings for that device, and then select the plus ("+") icon.

6 Repeat step 5 for each device that does not use the default mapping.

7 Select *OK*.

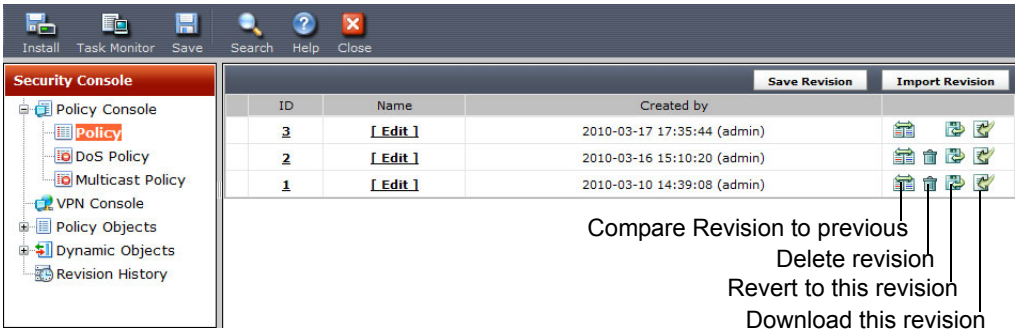
Revision History

The Security Console also includes a revision history. This enables you to view, compare and revert to previous installed configurations. This is very useful should an update to a device fail, due to a configuration error. You can simply revert to the previous version before the changes, and review the configuration.

To view the Revision History go to *Security Console* > *Revision History*. Alternately, if you have detached the *Security Console*, selecting the *Save* button brings you to the Revision History window. See "Security Console window" on page 197.

There must be changes since the last revision before you can create a new revision. If you attempt to create a new revision without any changes, nothing will happen.

Figure 138: Revision history in the Security Console



ID	The revision counter.
Created by	The date and time the revision was created, and the administrator/user who created it.

Installation	The installation status of the revision, and when it occurred.
Save Revision	Select to save the current ADOM revision.
Compare Revision	Select see what changes occurred between the current installation and the previous version. Select this option, select which revisions to compare, and the differences will be displayed in a separate window using red to indicate deleted sections, green to indicated new sections, and yellow to indicate modified sections.
Delete Revision	Select to remove the installation revision from the table. The current installed version will not have the icon available.
Revert to Revision	Select to install the revision on the devices. This will overwrite the current installation on the devices.
Download this Revision	Select to download the configuration for this revision as a file to your computer. The file downloaded is a plain text file.

Administrative Web Portal

As a security service provider, you can provide an administrative web portal for customers who have a requirement of managing, to some extent, their network security options. The portal can enable customers to control their own SSL VPN user list, Web Filter, URL filters, and categories. They can also view the firewall policies on their unit or VDOM.

Note: Administrative web portals are available when the FortiManager unit is running in EMS mode.

You create a portal profile and include the content and appearance of the web portal and can create more profiles if customers have differing needs. The portal is composed of selected configuration and monitoring widgets, on one or more pages, to provide the specific functionality that the administrators need to monitor their network security. You can also customize the web portal with a logo and select the colors and page layouts for your business, or match the customer's corporate look. With FortiManager, you define each customer/administrator as a portal user, assigned a specific device or VDOM and a portal profile.

Using FortiManager, you can maintain a number of FortiGate units and/or VDOMs for a large number of clients. These clients may also want to monitor and maintain their own firewall policies and traffic.

Customers access the web portal through the IP or URL of the FortiManager system. They log in the same way as the FortiManager administrator, using their own user name and password, created by the FortiManager administrator. Once logged in, the customer is directed to their assigned web portal. The customer never sees the FortiManager web-based manager or can configure it.

To create a web portal for customers to access, you need to first create a portal profile. A web portal is similar to a group. The profile is associated with a FortiGate unit, and if required, a VDOM configured on a specific FortiGate unit. Once set up, portal users, or administrators, can be added to the portal.

The following table lists the number of supported portals and portal users on each FortiManager model.

Table 11: Supported web portals and web portal users

FortiManager Model	Maximum portal	Maximum users
100C	10	200
400A and 400B	10	200
1000C	50	500
3000	50	500
3000C	100	4000
5001A	100	4000

After creating a web portal, you can configure it to add components that the user or administrator can review and modify as required. You can return at anytime to add and remove components from the portal. It is a good idea to meet or discuss with your users which components they would like to see on their portal. Provide them a list of what options they have, and allow them to select from the list.

The web portal can also be customized to a selection of color schemes, and you can add a user's logo to make the portal to fit the customer's corporate look. Users are not able to modify the layout or look of the web portal, although they can add and modify the content of some of the components. For example, they can add SSL-VPN users, modify URL filter lists, and add text notes. If they require changes to the components (adding or removing) or the layout of the components on the portal page, they will need to contact you.

Creating a web portal

Before creating a web portal, ensure you have the FortiGate configured and any VDOMs enabled and configured. You may also want to discuss with your user as to what components they want or required for their portal.

To create a web portal profile

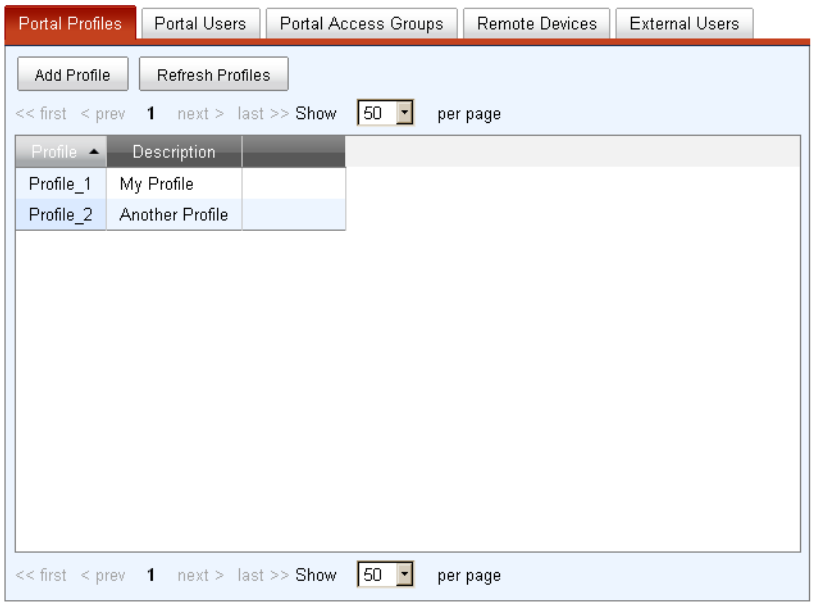
1. Go to *Device Manager* > *Web Portal* and select *Add Profile*.
2. In the *Profile* field, enter a name for the profile, and optionally, enter a *Description.*
3. If you have already added a portal profile you can select *Clone from existing profile* to add the new profile using the settings from a previously added profile.
4. Select *OK*.

The *Profile* name can be a maximum of 35 characters.

Configuring the web portal profile

With the web portal added, you can configure the portal with the available widgets. The selection of widgets are dependent on the FortiGate device and VDOM (if selected), that is, you may have more or less widgets available to choose from depending on the FortiGate device selected for the portal. The selected device is only used for assistance. The device or VDOM is defined when creating the user.

Figure 139: Web portal list



To configure the web portal profile

1 Go to *Device Manager* > *Web Portal*.

2 Select a profile from the list.

3 Select the *Configure Profile* icon for the profile.

4 You can optionally do the following to assist with editing the portal layout by including some real data in the portal. This is for display and editing purposes only.

- Select the type of *Remote Device*.
- Select the name of a *Device* added to the FortiManager configuration.
- Select a FortiGate unit and if required, a VDOM.

5 Select FortiAnalyzer options if required.

6 Select *Configure Profile*.

When you select *Configure Profile*, the web portal design window opens in a new window or tab of the browser. You may need to allow pop ups for the FortiManager IP or URL to allow the portal design window to appear, otherwise this window will not appear.

Modifying the content and layout

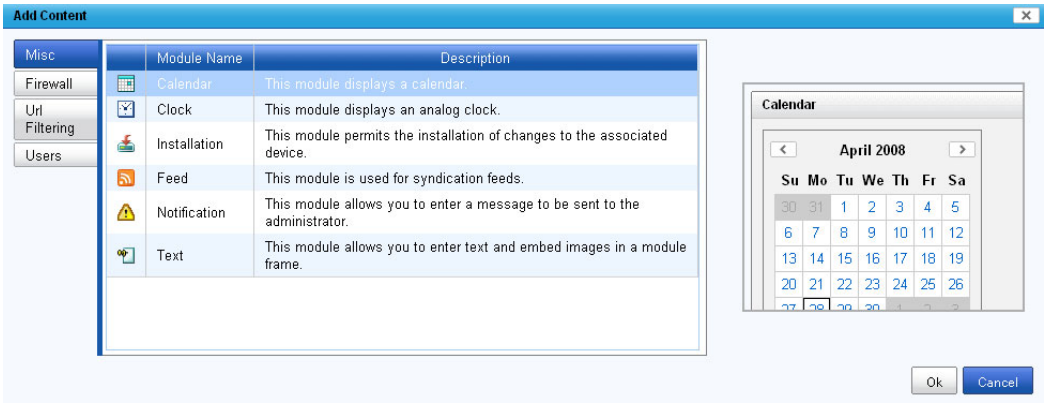
The web portal design window enables you to add content for the user's internet and firewall connection and arrange the layout of the information.

Before adding widgets for the portal, you will want to set up the portal window. There are a number of customizations you can do to the window including:

- change the name of the *Home* tab by clicking the name.
- select the number of columns for the page by selecting the *Edit Page Preferences* icon next to the page name.
- add more pages by selecting the *Add page* tab. Additional page tabs will appear at the top of the page window.

To add content, select *Add Content*.

Figure 140: Adding web portal content



A number of content options are available, with slight variation, depending on the FortiGate unit selected when setting up the web portal. Select a tab on the left to view the widgets available. To add a particular widget, either double-click to add the content, or select a widget and select *OK*. Holding the Control or Shift keys enables you to select multiple widgets.

Widgets available for the web portal include:

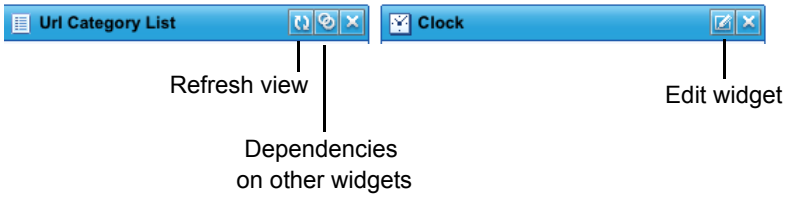
- Installation
- Run Report
- Firewall Policies
- Notification
- Text Messages
- URL Category List
- URL Filter List
- Local URL Category List
- Local URL Category Rating List
- SSL User Groups
- SSL User List

Once you have selected the widgets, you can move them on the page within the column chosen column view.

Tip: You can change the width of the columns. When you move your cursor between the widgets, you will see a line appear, demarcing the column borders. Click and drag left or right to expand or contract the column width.

Many of the widgets are configurable. In the title bar of the widgets, if there is an *Edit* or *Dependencies* icon on the right, further configuration can be done with the widget.

Figure 141: Widget title bar options

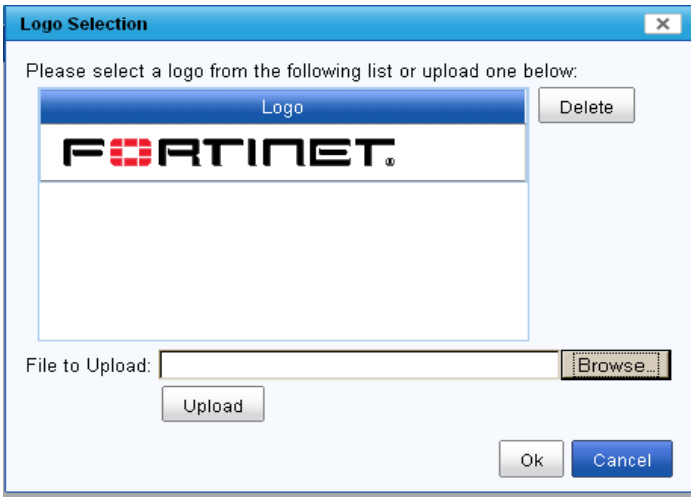


Tip: You can resize the widgets vertical size by clicking and dragging the bottom of the widget.

Adding a logo

You can add a logo to the web portal page. The logo can be your logo, or the logo of the user as a part of the customization to go with the color selection. The logo must be a bitmap image. It can be any size, color or monochrome. The logo file can be .jpg, .png, .bmp or .gif. Remember if the logo is too large or detailed, it may take longer for the portal page to load.

Figure 142: Adding a logo to the web portal



To add a logo to the web portal display

1. Select *Logo Preferences.*
2. Select *Browse* and locate the logo on your hard disk or network volume.
3. Select *Upload*.
4. Select the uploaded logo and select *OK*.

Portal Preferences

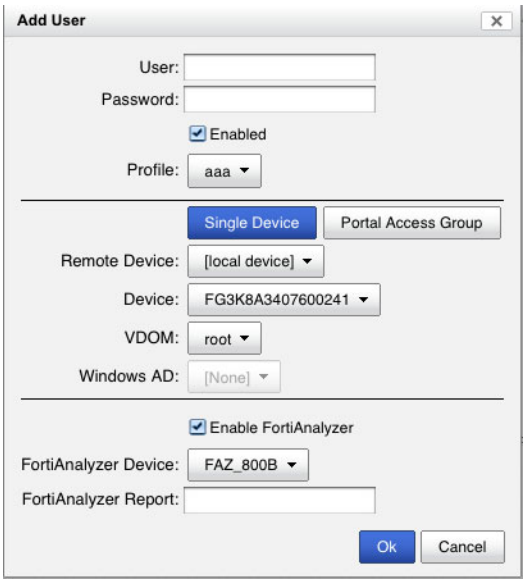
You can change the colors of the display from a list of color themes. To change the colors of the web portal display, select *Portal Preferences*, select the desired color scheme from the list, and select *OK.*

Creating a portal user account

To create a portal user account, go to *Device Manager* > *Web Portal* > *Portal Users* and select *Add User*. The *Add User* dialog opens. Enter or select the following items and select *OK*.

Note: The user name can be up to 35 characters and the password up to 20 characters.

Figure 143: New User dialog



User	Enter the name of the user who will log into the portal.
Password	Enter the password for the user.
Enabled	Select to enable the user profile.
Profile	Select the profile for this user from the list.
Device	Select the device that the user will administer.
VDOM	Select the VDOM that the user will administer. Only available if virtual domains are enabled on the FortiGate device.
Enable FortiAnalyzer	Select to enable FortiAnalyzer reporting for the FortiGate device.
FortiAnalyzer Device	Select the FortiAnalyzer Device that will create the reports.
FortiAnalyzer Report	Enter a name for the report generated by the FortiAnalyzer device.

Portal access groups

Portal access groups is a way to provide portal users who need to monitor or maintain multiple FortiGate units or VDOMs, a way to maintain them without having to log in multiple times for each device. It provides a one-stop location.

By creating a portal access group, you add two or more devices/VDOMs, local or remote to the group. The group is then applied to a portal user.

To create a portal access group

1 Go to *Device Manager* > *Web Portal* > *Portal Access Groups*.

2 Select *Add Portal Access Group*.

3 Enter the following and select *OK*:

Group	Enter a name for the group.
Description	Enter a description for the group.
Remote Device	Select a FortiGate unit from the list.

VDOM	If there are VDOMS for the selected FortiGate unit, the list will become active for you to select a VDOM.
Windows AD	If the VDOM employs Windows Active Directory authentication, the list will be come active for you to select a user.
Alias	Enter an alias name for the FortiGate unit that will be more meaningful than the FortiGate unit serial number that appears for the *Remote Device*. Select *Add* to add the Alias. You can add multiple aliases.

When the portal user logs into their web portal, an additional widget appears on the web page called Device Navigator.

Figure 144: Web portal with multiple devices

The widget displays the alias of the FortiGate unit or VDOM that the other widgets are displaying information for. By selecting the *Navigate* button in the widget title bar, the list of other FortiGate units or VDOMs available for that portal user appears. The portal user can select the desired alias name and select *Switch* to view the information for the FortiGate unit or VDOM.

Remote devices

Use the Remote device tab for adding remote FortiManager units so that a portal user can be bound to a device on one of the remote units. This allows a second FortiManager unit to be behind a firewall that does the actual management of the FortiGate units, and have another more public FortiManager unit supporting the interface for the portal users. The remote device requires external users configured so proper authentication can be made between the two (or more) remote FortiManager units.

To add remote devices

1 Go to *Device Manager* > *Web Portal* > *Remote Device*.

2 Select *Add Remote Device*.

3 Enter the following and select *OK*:

Name	Enter a name for the FortiGate unit.
Description	Enter descriptive information about this device.
Address	Enter the IP address for the FortiGate unit.
User	Enter a user name for administrative login
Password	Enter a password for the user.

External users

Use the *External Users* tab to add users in conjunction with the *Remote Devices* configuration. This enables users to have remote access to the managing FortiManager unit from the portal FortiManager unit.

You also use external users when creating custom widgets that you can add on custom portal web pages or web portals such as iGoogle.

To add external users

1 Go to *Device Manager* > *Web Portal* > *External Users*.

2 Select *Add External User*.

3 Enter the following and select *OK*:

User	Enter a name for the FortiGate unit.
Password	Enter a password for the user.

Using the web portal

The purpose of the web portal is to enable customers, or their administrators the ability to monitor and maintain their firewall settings.

Before the users can use the web portal you need to supply them with the following information:

- the URL or IP address of the FortiManager system
- the user name
- the user password

The user enters the FortiManager system URL or IP address into the web browser. When they get the login screen, they enter the supplied user name and password. This will log them into the portal site, displaying the colors, widgets and arrangements setup from the previous steps.

The administrator can view firewall information, maintain and update information depending on the widgets included for the portal. The user can log out of the portal by selecting the *Logout* button in the upper right corner of the browser window.

Configuring Devices

Use the *Device Manager* window to configure the devices that you have added. For more information on adding devices, see “Managing Devices” on page 81.

This section focuses on FortiGate configuration using the FortiManager system. There are some tasks that cannot be performed or are performed differently on a FortiGate unit using the FortiGate web-based manager. For FortiAnalyzer configuration, once you select a FortiAnalyzer unit in the *Device Tree*, the web-based manager for the unit displays. For more information about FortiAnalyzer settings and configuration, see “FortiAnalyzer Devices” on page 299 and the ***FortiAnalyzer Administration Guide***.

For information about how installation and configuration features interact with each other, see “Configuration and installation workflow” on page 18.

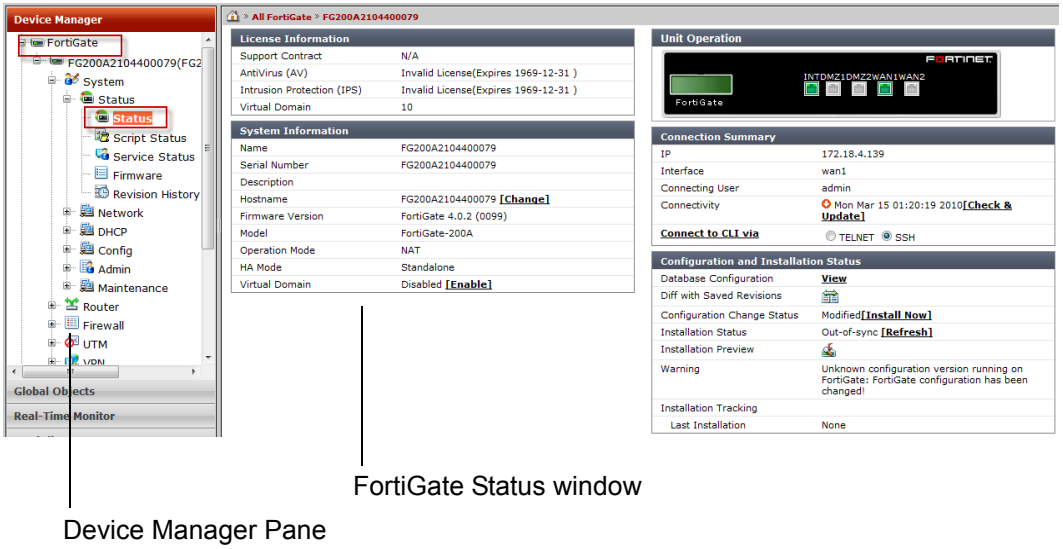
This section contains the following topics:

Device Manager pane

To view and change FortiGate configurations while in the *Device Manager* pane, select a FortiGate unit in the *All FortiGate* window. For more information about the Device Manager window, see “Device Manager window” on page 81.

The FortiGate unit’s Status window opens. The items in the FortiGate menu that are mostly identical to the options you would see on the native FortiGate Navigation Pane.

Figure 145: Device Manager pane with FortiGate unit menu



Configuring devices

You can configure the FortiGate units in two ways:

- By selecting a single device from the *Device Manager*, you can configure the settings of this device.
- By selecting a virtual domain (VDOM) from the *Device Manager*, you can configure settings for that virtual domain.

Note: If you see padlock icons beside the devices in the Navigation Pane, it means that device locking is enabled. Before you can make any configuration changes to a device, you must lock the device to avoid configuration conflicts with other administrators. For more information on device locks see "Device configuration locks" on page 69.

This section contains the following topics:

Configuring a device

Configuring a FortiGate unit using the *Device Manager* pane is very similar to configuring FortiGate units using the FortiGate web-based manager. You can also save the configuration changes to the configuration repository and install them to other FortiGate unit(s) at the same time. For more information, see "Managing configuration revision history" on page 278.

This document does not provide detailed procedures for configuring FortiGate units. See the FortiGate documentation for complete information. Complete FortiGate documentation is available from the FortiManager system CD. The most up-to-date FortiGate documentation is also available from Fortinet Technical Support.

Note: If you see padlock icons beside the devices in the Navigation Pane, it means that device locking is enabled. Before you can make any configuration changes to a device, you must lock the device to avoid configuration conflicts with other administrators. For more information on device locks see "Device configuration locks" on page 69.

To configure a FortiGate unit

1. In the *Device Manager* pane, select the unit you want to configure.
2. Select an option (such as System, Router, Firewall, UTM, VPN, User, Endpoint Control, or Log&Report) for that unit in the Device Manager pane.
3. Configure the unit as required.

   The configuration changes are saved to the FortiManager device database instead of the FortiManager repository represented by the *Revision History* window.

Note: You can rename and reapply firewall objects such as address, address group, service, schedule, VIP, load balance, protection profile, and traffic shaping after they are created and applied to a firewall policy. When you do so, the FortiManager system will:

- delete all dependencies such as the firewall policy
- 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 WebUI, 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 web-based 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.

Configuring virtual domains (VDOMs)

Virtual domains (VDOMs) enable you to partition and use your FortiGate unit as if it were multiple units. For more information see the *FortiGate Administration Guide* or the *VLAN and VDOM Guide*. VDOMs are only available on units running FortiOS V3.0 or higher.

To view the VDOM list, in the FortiGate menu of a device, select *System* > *Virtual Domain* > *Virtual Domain*.

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 click 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. For more information, see "Configuring VDOM resource limits" on page 220 and "Configuring VDOM global resources" on page 221.

Creating and editing virtual domains

Creating and editing virtual domains in the Fortimanager system is very similar to creating and editing VDOMs using the FortiGate web-based manager.

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

To enable virtual domains

1. In the *Device Manager* pane, select the unit you want to configure.
2. In the FortiGate menu of a device, select *System* > *Status* > *Status*.
3. In the *System Information* area, click the *Enable* link in the *Virtual Domain* field.

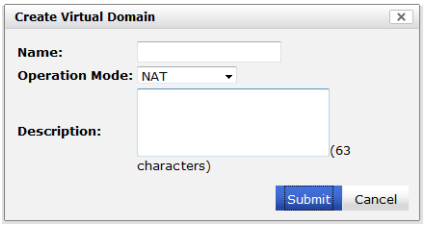
To create a virtual domain

1 In the *Device Manager* pane, select the unit you want to configure.

2 In the FortiGate menu, select *System* > *Virtual Domain* > *Virtual Domain*.

3 Click *Create New*.

Figure 146: Creating a VDOM



4 Enter the name, operation mode and an optional description for the new VDOM. If you select Transparent mode you will also need to enter the management IP and mask as well as the gateway.

5 Click *Submit* to create the new VDOM.

The new VDOM will appear in the list.

Configuring VDOM resource limits

A VDOM's resource limit defines how much resources a VDOM can consume. You can set a VDOM's maximum and guaranteed limits for each resource. You can also view the current usage of the resources by the VDOM.

A VDOM's maximum limit for a resource cannot be greater than the global maximum limit set for this resource. This value is not guaranteed if you have more than one VDOM with each one having a maximum limit value and all are running at the same time.

A VDOM's guaranteed resource limit is the actual amount of resource a VDOM can use regardless of the number of VDOMs running at the same time. Although each VDOM can have its own guaranteed limit, the sum of guaranteed resource limits for all VDOMs must be less than or equal to the global maximum resource limit.

For more information, see "Configuring VDOM global resources" on page 221.

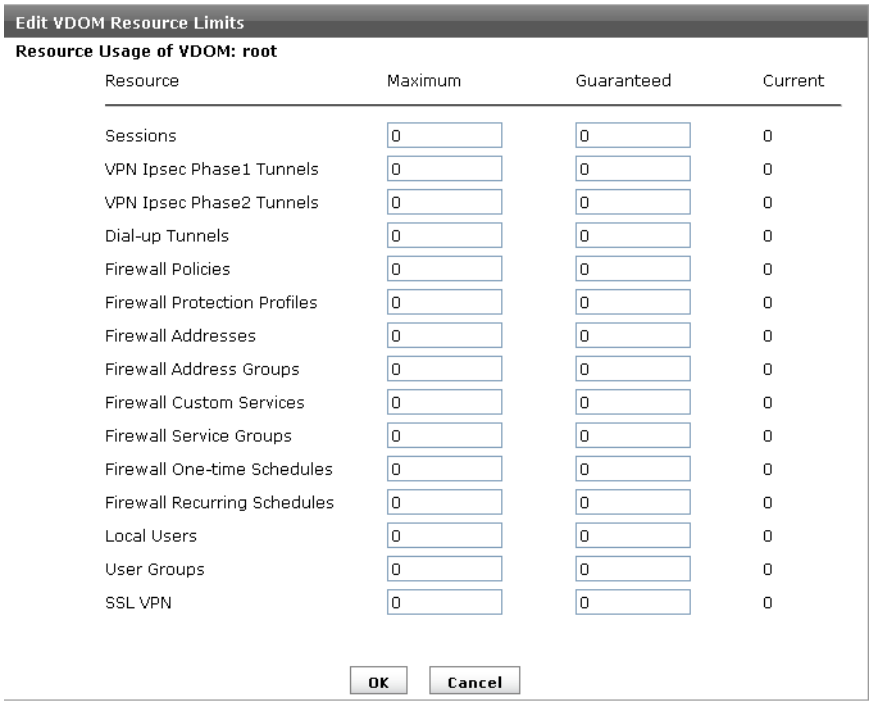
To configure a VDOM's resource limits

1 In the *Device Manager* pane, select the unit you want to configure.

2 In the FortiGate menu, select *System* > *Virtual Domain* > *Virtual Domain*.

3 Click the *Resource Limit* icon of a VDOM.

Figure 147: Configuring VDOM resource limits



4 For each resource:
   - enter the maximum value allowed for this resource. If you enter a wrong value, a warning appears with the correct value range.
   - enter the value allocated for this resource. This value must be lower than or equal to the maximum value.

5 Click *OK*.

Configuring VDOM global resources

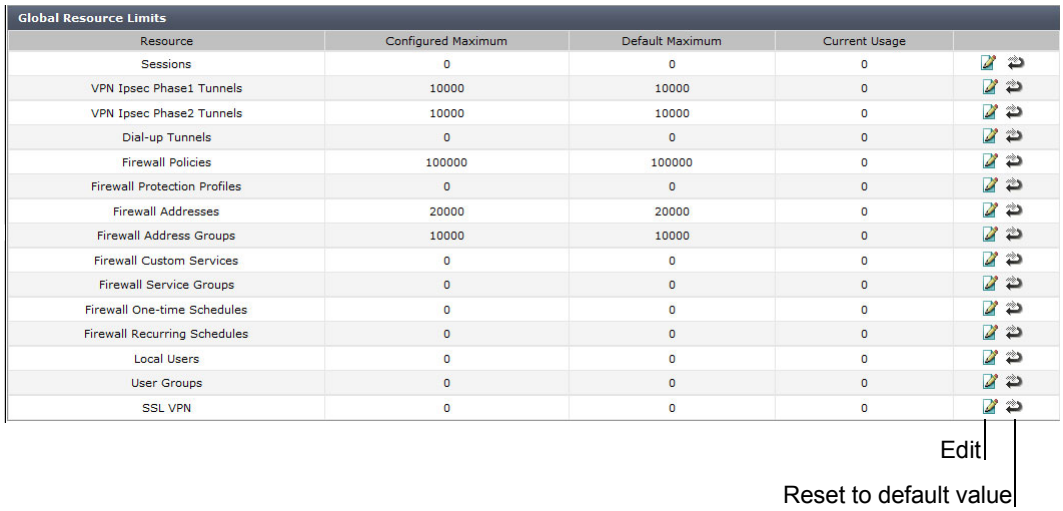
You can set a maximum limit for each resource that each VDOM in a device can consume. Each VDOM's maximum limit cannot exceed the global maximum limit set for the same resource. This is a good way to allocate network resources.

To configure VDOM global resources

1 In the *Device Manager*, select the unit you want to configure.

2 In the FortiGate menu, select *System* > *Virtual Domain* > *Global Resources.*

Figure 148: Configuring VDOM global resources



Resource	The network resources that the VDOMs can use.
Configured Maximum	The maximum resource limit for all VDOMs set by the user. For more information, see “Edit icon” on page 222.
Default Maximum	The default maximum resource limit for all VDOMs.
Current Usage	The total consumption of the resource by all VDOMs.
Edit icon	Select to set a maximum resource limit for all VDOMs.
Reset to default value	Select to set the configured maximum limit to the default maximum limit.

Installing configuration changes

After making device configuration changes, you can install them to the selected devices at the same time. For more information, see “Installing Device Configurations” on page 277.

•

Working with Scripts

FortiManager scripts enable you to create, execute and view the results of scripts executed on FortiGate devices attached to the FortiManager system. At least one FortiGate device must be configured on the FortiManager system for you to be able to use scripts. Scripts can also be run on the FortiManager global database.

Note: 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. The first format contains 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.

The second format uses 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 easily reduce the troubleshooting required for your scripts.

This section contains the following topics:

For information about scripting commands, see *FortiGate CLI reference*.

Note: Before using scripts, ensure the `console more` function has been disabled in the FortiGate CLI. Otherwise scripts and other output longer than a screen in length will not execute or display correctly.

Device View

While in Device Manager, select a FortiGate device and select *System* > *Script Status*. This is the script status page for that device, or the default script view. This page shows all the scripts loaded into the device and also shows schedules for executing them and script execution history.

This is different from the Script Repository where all the scripts on your FortiManager system are listed, not just scripts for one device or group. Go to *Device Manager* > *Script* to view scripts available for all devices. For more information, see "Script View" on page 226.

Note: If you see padlock icons beside the devices in the navigation frame, it means that device locking is enabled. Before you can make any configuration changes to a device, you must lock the device to avoid configuration conflicts with other administrators. For more information on device locks see "Device configuration locks" on page 69.

Individual device view

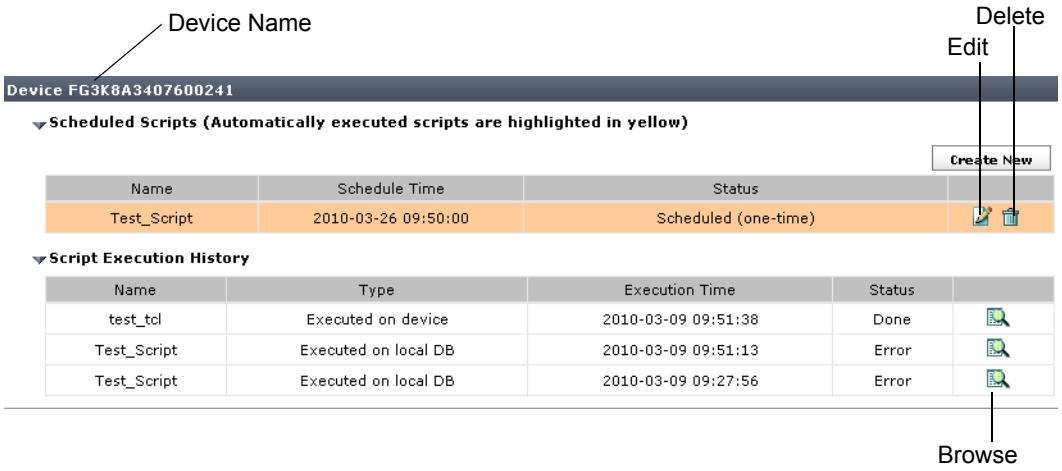
From the initial Device Manager view, of an individual device, selecting the *System* > *Script Status* brings you to the script view for that device.

From the initial Device Manager view, of a device group, selecting the *<group_name>* > *Script* brings you to the script view for that device group.

The name of the device or device group displayed at the top of the screen. This view has two sections: scheduled scripts, and script execution history.

To create a new schedule to execute a script, see "To schedule a script" on page 225.

Figure 149: Individual Device View



Scheduled Scripts	Select the arrow to expand or collapse this section. For more information on scheduling scripts, see "Scheduling a script" on page 225.
Create New	Select to schedule the execution of a script on this device. For more information on scheduling scripts, see "Scheduling a script" on page 225. This button appears only if you lock the device.
Name	The name of the script that has been scheduled to execute on this device.
Schedule Time	The date and time this script is scheduled to execute. If it is a recurring schedule, additional information such as the day of the week is displayed here. Based on the type of script schedule, the following information is displayed: • One-time - date and time the script will execute • Recurring daily- time the script will execute. • Recurring weekly - weekday and time the script will execute • Recurring monthly - day of the month and time the script will execute • Automatic - this row has a yellow background, but no text is displayed. The script will only execute when the configuration on the device or group is installed.
Status	The type of schedule for this script - either Scheduled or Automatic. Scheduled can be one of one-time, recurring daily or recurring monthly.
Edit icon	Select to modify the schedule for the script. You can change it to *Execute Now*, *Scheduled* or *Automatic* as well as changing the schedule information.
Delete icon	Select to cancel the scheduled script.
Script Execution History	Select the arrow to expand or collapse this section.

Name	The name of the script that was executed on this device.
Type	Specifies whether the script was executed on the local FortiManager database or on the device or device group.
Execution time	The date and time when the script ran.
Status	The status of the script execution. Status is *Done* if the script executed correctly and *Error* if the script encountered an error and couldn't finish.
Browse icon	Select to view the Script History. This is the output that was displayed during the execution of the script and will include error information if an error has occurred.

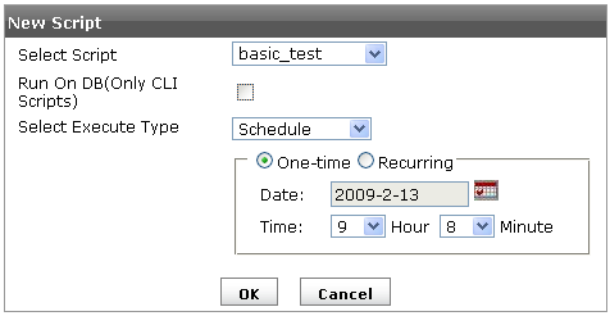
Scheduling a script

From the individual or group device views, you can select *Create New* to schedule one or more existing scripts to execute on that device or group.

Scheduling a script on a group of devices is the same as for a single device, except that you can exclude devices from the group. These excluded devices will not execute this scheduled script.

Note: If you see padlock icons beside the devices in the navigation frame, it means that device locking is enabled. Scripts that change the configuration will not execute on unlocked devices. Before you can make any configuration changes to a device, you must lock the device to avoid configuration conflicts with other administrators. For more information on device locks see "Device configuration locks" on page 69.

Figure 150: Scheduling a script



To schedule a script

1. Go to D*evice Manager*, select the device and select *System* > *Script Status*.

   For a device group, select the device group and select *Script*.
2. Select *Create New*.
3. Select a script from the *Select Script* list. If there are no scripts in this list, create a new script. For more information, see "Creating or editing a script" on page 227.
4. Select *Run On DB (Only CLI Scripts)* to have your script run on the FortiManager device database instead of directly on the managed device. This option is not available for Tcl scripts.
5. Select the Execute Type as one of:
   - Execute now - runs the script on the device when you select OK.
   - Schedule - displays additional options for selecting the type of scheduling, date, and time.
   - Automatic - the script will execute when the configuration on this device or group is committed or deployed.

6 Select scheduling information as required.
   - For a *One-Time* schedule, select the calendar icon to browse calendar months to quickly select the month and day of the month.
   - For a *Recurring* schedule, select the type as one of daily, weekly or monthly. For weekly, select the day of the week to run the script. For monthly, select the day of the month to run the script. Select the hour and minute to run the script on that day. Hours are based on the 24-hour clock.
7 For a group of devices, optionally select which devices in the group to exclude.
8 Select *OK* to save this script schedule, and return to the device or group view.

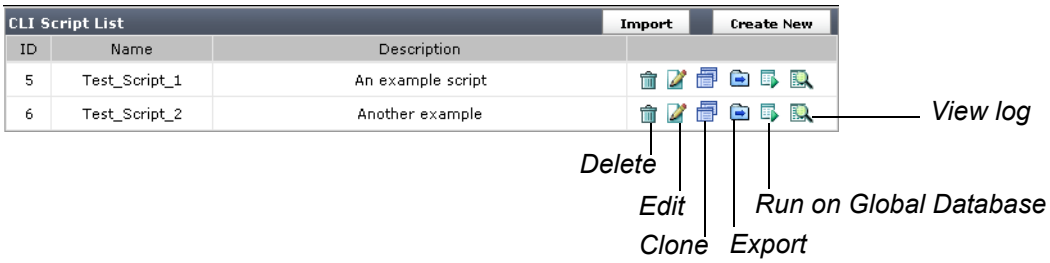
Script View

You can use the Device Manager script Repository to add, clone, edit, delete, and export scripts. You can also execute CLI scripts on the global database and view the results of running the script.

To view the list of scripts, go to *Device Manager* > *Script*. You can select *CLI Script, CLI Script Group*, or *Tcl Script*. CLI scripts only allow you to use Fortinet CLI commands in your script. Tcl scripts allow you to use Tcl scripting language commands which can include CLI commands as well. CLI Script Group is grouping some scripts together that will be run, making it easier to schedule multiple scripts at one time.

When you are creating, editing, or deleting scripts you are working in the Script Repository.

Figure 151: CLI Script Repository



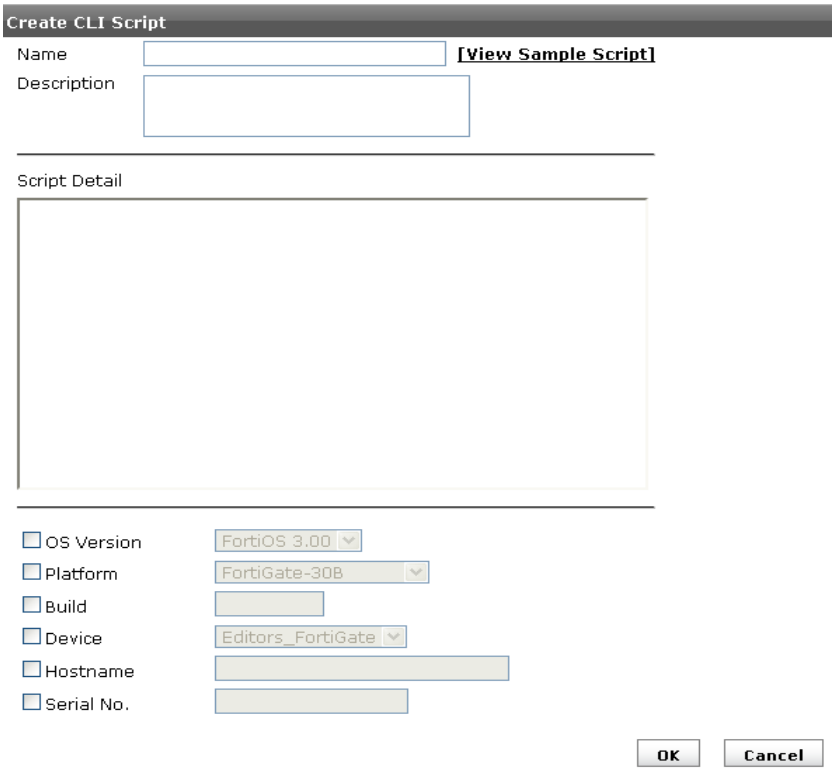
Import	Select to import a script. The script will be imported from a plain text file on your local computer.
Create New	Select to create a new script. For more information, see “Creating or editing a script” on page 227.
ID	The ID assigned to this script.
Name	The name of the script. The script name can include spaces, but cannot include punctuation.
Description	A brief description of the script.
Delete icon	Select this icon to delete this script. If this icon does not appear, the script is in use and cannot be deleted at this time. Generally this indicates the script has been scheduled to run on a device at a later date.
Edit icon	Select to view or change the script information.
Clone icon	Select to create a duplicate of this script with another name. For more information, see “Cloning a script” on page 228.
Export icon	Export a script in the form of a text file that you can download to your PC. The default name of the file is script.txt.

Run on Global Database icon	Select to run this script on the FortiManager global database. Only CLI scripts can be run on the global database, and the CLI commands must be the full command, no short forms.
View Log icon	Select to view the log of this script running on the global database. Select *Return* to come back to this screen when done.

Creating or editing a script

From the Device Manager script screen, you can create a new script or edit an existing script.

Figure 152: Create or Edit a script



To create or edit a script

1. Go to *Device Manager* > *Script* and select either *CLI Script* or *TCL Script*.
2. Select either *Create New* or select the *Edit* icon for the script to edit.
3. If you are creating a script, enter a short descriptive name for this script. The name should be unique and easy to recognize. If you are editing an existing script, the script name is read-only.

   For tips and examples on how to write scripts, select the *View Sample Script* link to open a small online help window that contains various script examples.
4. Enter a description of what action(s) the script performs. As with the script name, keep the description short and useful.

5 Enter your script in the *Script Detail* field by:
- entering the commands manually (for CLI or Tcl scripts)
- cutting and pasting from a FortiGate unit CLI (for CLI scripts)
- cutting and pasting from an editor of your choice (for CLI or Tcl scripts)

For information on writing CLI or TCL scripts, see "Script Samples" on page 229.

Note: When creating a script, use full command syntax instead of abbreviations.

Note: For longer Tcl scripts, a context sensitive editor is recommended to reduce errors.

Note: Tcl scripts cannot include the Tcl exit command.

6 Optionally you can add information to limit what devices can run the script. This includes selecting the FortiOS version, the FortiGate platform, which firmware build, the device name, the hostname of the device, and the serial number.

7 Select *OK* to save your new script and return to the Script Repository.

After creating or editing a script, you can test it using the script procedure in "Scheduling a script" on page 225. If your script does not execute properly, see "Script Samples" on page 229 for troubleshooting tips.

Cloning a script

Cloning is a fast way to create a new script that shares some commands with an existing script. It can avoid typos and be easier than cutting and pasting.

To clone a script

1 Go to *Device Manager* > *Script*, select either *CLI Script* or *TCL Script*, and select the *Clone* icon for the script you want to duplicate.

2 Enter a new name for the duplicate script.

By default it is given the same name as the original script with the prefix of "copy_", so a script called "test" would result in a default duplicate called "copy_test".

3 Optionally enter a new description.

It is recommended to change the description when cloning. This is another method to ensure the original the cloned scripts are not confused for each other.

4 Edit the script to make the necessary changes.

5 Save your new script.

Exporting a script

You can export scripts as text files.

To export a script

1 Go to *Device Manager* > *Script*, select either *CLI Script* or *TCL Script*, and select the *Export* icon for the script you want to export.

2 Download the text file to your PC.

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

Note: 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 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 can not 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 232.

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 233.

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.

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

To view information about all the configured FortiGuard Distribution Network (FDN) servers on this device

Script
```
diag debug rating
```

Output
```
Locale       : english

The service is not enabled.
```

Variations Output for this script will vary based on the state of the FortiGate device. The above 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.

Note: 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.

To create a new account profile called policy_admin allowing read-only access to policy related areas

Script

```
config system accprofile
   edit "policy_admin"
      set avgrp read
      set fwgrp read
      set ipsgrp read
      set loggrp read
      set spamgrp read
      set sysgrp read
      set webgrp read
   next
end
```

Output

```
Starting script execution
config system accprofile

(accprofile)# edit "policy_admin"
set avgrp read
set fwgrp read
set ipsgrp read
set loggrp read
set spamgrp read
set sysgrp read
set webgrp read
next
end

exit
new entry 'policy_admin' added
(policy_admin)# set avgrp read
(policy_admin)# set fwgrp read
(policy_admin)# set ipsgrp read
(policy_admin)# set loggrp read
(policy_admin)# set spamgrp read
(policy_admin)# set sysgrp read
(policy_admin)# set webgrp read
(policy_admin)# next
(accprofile)# end
MyFortiGate #
MyFortiGate #
MyFortiGate # exit
```

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 privileges 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 firewall policy
  edit 1
    set srcintf “port1”
    set dstintf “port2”
    set srcaddr “all”
    set dstaddr “all”
    set status disable
    set schedule "always"
    set service "ANY"
    set logtraffic enable
    set status enable
   next
end
```

- Running a CLI script on the global database

```
config firewall policy
  edit 1
    set _global-srcintf "port1"
    set _global-dstintf "port2"
    set srcaddr "all"
    set dstaddr "all"
    set status disable
    set schedule "always"
    set service "ANY"
    set logtraffic enable
    set status enable
    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 mature 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.

Note: Do not include the exit command that normally ends Tcl scripts—it will cause the script to not run.

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 web site 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 three areas:

- Tcl variables
- Tcl loops
- Tcl decisions

- Tcl file IO

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. For more information on the limitations of FortiManager Tcl, see your Release Notes, and the Fortinet Knowledge Center.

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.

Note: 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.

To save system status information in an array

Script

```
#!
proc get_sys_status aname {
   upvar $aname a
   set input [exec "get system status\n" "# "]
   set linelist [split $input \n]
   foreach line $linelist {
       if {![regexp {([^:]+):(.*)} $line dummy key value]} continue
       switch -regexp -- $key {
           Version {
                regexp {Fortigate-([^ ]+) ([^,]+),build([\d]+),.*} $value dummy a(platform) a(version) a(build)
           }
           Serial-Number {
               set a(serial-number) [string trim $value]
           }
           Hostname {
               set a(hostname) [string trim $value]
           }
       }
   }
}

get_sys_status status

puts  "This machine is a $status(platform) platform."
puts  "It is running version $status(version) of FortiOS."
puts  "The firmware is build# $status(build)."
puts  "S/N: $status(serial-number)"
puts  "This machine is called $status(hostname)"
```

Output

```
Starting script execution

This machine is a 100A platform.
It is running version 2.80 of FortiOS.
The firmware is build# 318.
S/N: FGT0172020120181
This machine is called techdocs-100A.
```

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 {$status(version) == 3.0} {
# follow the version 3.0 commands
} elseif {$status(version) == 4.0} {
# follow the version 4.0 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 regexp command and based on a match, performs one of the actions listed in lines 9 through 17
- lines 9-11 if regexp 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 regexp 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 regexp is matched against 'Hostname'
- line 17-19 close the switch decision statement, the foreach 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.

To create 10 users from usr0001 to usr0010

Script

```
1  #!
2  proc do_cmd {cmd} {
3  puts [exec "$cmd\n" "# " 15]
4  }
5  set num_users 10

6  do_cmd "config user local"
7  for {set i 1} {$i <= $num_users} {incr i} {
8  set name [format "usr%04d" $i]
9  puts "Adding user: $name"
10 do_cmd "edit $name"
11 do_cmd "set status enable"
12 do_cmd "set type password"
13 do_cmd "next"
14 }
15 do_cmd "end"

16 do_cmd "show user local"

17
```

Output

```
Starting script execution
config user local
(local)#
Adding user: usr0001
edit usr0001
new entry 'usr0001' added
(usr0001)#
set status enable
(usr0001)#
set type password
(usr0001)#
next

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

Fortigate-50A #
show user local

config user local
    edit "usr0001"
        set type password
    next
    edit "usr0002"
        set type password
    next
end

Fortigate-50A #
```

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 username 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. For example you can execute different versions of a script depending on if the Fortigate device is executing FortiOS version 2.8, version 3.0, or version 4.0.

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.

To add information to existing firewall policies

Script

```
1  #!
2  # need to define procedure do_cmd
3  # the second parameter of exec should be "# "
4  # If split one command to multiple lines use "\" to continue


   proc do_cmd {cmd} {
5    puts [exec "$cmd\n" "# "]
6  }
   foreach line [split [exec "show firewall policy\n" "# "] \n] {
7    if {[regexp {edit[ ]+([0-9]+)} $line match policyid]} {
       continue
8    } elseif {[regexp {set[ ]+(\w+)[ ]+(.*)\r} $line match key
   value]} {
9      lappend fw_policy($policyid) "$key $value"
10   }
11 }
12 do_cmd "config firewall policy"
   foreach policyid [array names fw_policy] {
     if {[lsearch $fw_policy($policyid){diffservcode_forward
   000011}] == -1} {
13
14     do_cmd "edit $policyid"
15     do_cmd "set diffserv-forward enable"
       do_cmd "set diffservcode-forward 000011"
       do_cmd "next"
16   }
17 }
18 do_cmd "end"
19


20


21
```

Output

Variations This type of script is useful for updating long lists of records. For example if FortiOS version 3.0 MR4 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 foreach 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 foreach loop
- line 18 saves all the updated firewall policy entries

Additional Tcl Scripts

To get and display state information about the FortiGate device

Script

```
1  #!
2
3  #Run on FortiOS v3.00
4  #This script will display FortiGate's CPU states,
5  #Memory states, and Up time
6
7  set input [exec "get system status\n" "# "]
8  regexp {Version: *([^ ]+) ([^,]+),build([0-9]+),[0
9  -9]+} $input dummy status(Platform) status(Version)
10 status(Build)
11
12 if {$status(Version) eq "3.00"} {
13   puts -nonewline [exec "get system performance
14 status\n" "# " 30]
15 } else {
16   puts -nonewline [exec "get system performance\n" "#
17 " 30]
18 }
19
```

Output

```
Starting script execution

get system performance

CPU states:    92% used, 8% idle
Memory states: 55% used
Up:            9 days,  5 hours,  1 minutes.
Fortigate-50A #
```

Variations none.

Versions 3.0

To configure common global settings

Script

```
1  #!
2
3  #Run on FortiOS v3.00
4  #This script will configure common global settings
5  #if you do not want to set a parameter, comment the
6  #corresponding set command
7  #if you want to reset a parameter to it's default
8  #value, set it an empty string
9
10 set sys_global(ntpserver) "2.2.2.2"
11 set sys_global(admintimeout) ""
12 set sys_global(authtimeout) 20
13 set sys_global(ntpsync) "enable"
14
15 #procedure to execute FortiGate command
16 proc fgt_cmd cmd {
17   puts -nonewline [exec "$cmd\n" "# " 30]
18 }
19
20 #config system global---begin
21
22 fgt_cmd "config system global"
23 foreach key [array names sys_global] {
24   if {$sys_global($key) ne ""} {
25     fgt_cmd "set $key $sys_global($key)"
26   } else {
27     fgt_cmd "unset $key"
28   }
29 }
30 fgt_cmd "end"
31
32 #config system global---end
33
34
```

Output

```
Starting script execution
```

Variations none

To configure syslogd settings and filters

Script

```
#!

#Run on FortiOS v3.00
#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.
set filter_list {{attack enable} {email enable} {im
enable} {severity} {traffic enable} {virus disable}
{web enable}}

#set the number of syslogd server, "", "2" or "3"
set syslogd_no "2"

#procedure to execute Fortogate 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 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 script execution

config log syslogd2 setting
(setting)# set status enable
(setting)# set csv enable
(setting)# set facility alert
(setting)# unset port
(setting)# set server 1.1.1.2
(setting)# end
FGT# config log syslogd2 filter
(filter)# set attack enable
(filter)# set email enable
(filter)# set im enable
(filter)# unset severity
(filter)# set traffic enable
(filter)# set virus disable
(filter)# set web enable
(filter)# end
FGT#
```

Variations none

To 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 address-mode static
set encrypt enable
#localid will be set as the hostname automatically
#later
set psksecret "123456"
set server 1.1.1.1
set ver-1 disable

#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 address-mode encrypt localid
psksecret server ver-1}

#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 system fortianalyzer$faz_no"

foreach key $key_list {
  if [info exists $key] {
    fgt_cmd "set $key [set $key]"
  } else {
    fgt_cmd "unset $key"
  } }
fgt_cmd "end"
#config system fortianalyzer---end

```

Output

```
Starting script execution
config system fortianalyzer
(fortianalyzer)# set status enable
(fortianalyzer)# set address-mode static
(fortianalyzer)# set encrypt enable
(fortianalyzer)# set localid bob_the_great
(fortianalyzer)# set psksecret 123456
(fortianalyzer)# set server 1.1.1.1
(fortianalyzer)# set ver-1 disable
(fortianalyzer)# end
FGT#
```

Variations none

To create custom IPS signatures and add them to a custom group

Script

```
#!

#Run on FortiOS v3.00
#This script will create custom ips signatures and
#add them to a custom signature group

#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 group settings
set custom_rule(c1) {{status enable} {action drop}
{log enable} {log-packet} {severity high}}

set custom_rule(c2) {{status enable} {action reset}
{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 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 group custom---begin
fgt_cmd "config ips group custom"
foreach rule_name [array names custom_rule] {
  fgt_cmd "config rule $rule_name"
  set_kv $custom_rule($rule_name)
  fgt_cmd "end"
}
fgt_cmd "end"
#config ips group custom---end

```

Output

```
Starting script execution
config ips custom
(custom)# edit c1
new entry 'c1' added
(c1)# set signature "F-SBID(--protocol icmp; --icmp_type 10;
)"

(c1)# next
(custom)# edit c2
new entry 'c2' added
(c2)# set signature "F-SBID(--protocol icmp; --icmp_type 0;
)"

(c2)# next
(custom)# end
FGT# config ips group custom
(custom)# config rule c1
(c1)# set status enable
(c1)# set action drop
(c1)# set log enable
(c1)# unset log-packet
(c1)# set severity high
(c1)# end
(custom)# config rule c2
(c2)# set status enable
(c2)# set action reset
(c2)# unset log
(c2)# set log-packet disable
(c2)# set severity low
(c2)# end
(custom)# end
FGT #
```

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 filename 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 10 M 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

```
1  #!
2
3  set somefile {open “tcl_test” “w”}
4  puts $somefile "Hello, world!"
5  close $somefile
6
```

Output

Variations

Versions 3.0, 4.0

To read from a file

Script

```
1  #!
2
3  set otherfile {open “tcl_test” “r”}
4  while {[gets $otherfile line] >= 0} {
5      puts [string length $line]
   }
7  close $otherfile
8
```

Output

```
Hello, world!
```

Variations

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. Scripts that use FortiOS 3.0 commands will not work on devices running FortiOS 2.8. Likewise some scripts written for FortiOS 4.0 may not run on FortiOS 3.0.
- 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
  }
```

Using FortiGuard services

Note: FortiGuard services are available when in the administrative domain is in Element Management (EMS) mode. If you have added more than one administrative domain you can only configure FortiGuard services from the root administrative domain.

The Fortinet Distribution Network (FDN) provides FortiGuard services for your FortiManager system and its managed devices. The FDN is a world-wide network of Fortinet 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 antispam rating databases and lookups
- vulnerability scan and management support (FortiAnalyzer only)

To view and configure these services, go to *System Settings* > *FortiGuard Center* > *Configuration*. In FortiGuard Center, you can configure the FortiManager system to act as private FDS or use a web proxy server to connect to the FDN. FortiManager systems acting as a private FDS synchronize their packages with the public FDN, then provide FortiGuard updates and lookup replies to your private network's FortiGate units and FortiClient installations. This on-site FDS provides a faster connection, reducing Internet connection load and time required to apply frequent updates, such as antivirus signatures, to many devices. For example, you might enable service to FortiClient installations on the built-in FDS, then specify the FortiManager system's IP address as the override server on your FortiClient installations. Instead of burdening your Internet connection with all FortiClient installations downloading antivirus updates separately, the FortiManager system would use the Internet connection once to download the FortiClient antivirus update, then re-distribute the package to the FortiClient installations.

FortiGuard services also include updating firmware images. To view and configure firmware options, go to *System Settings* > *Firmware Images*. You can download these images from FDS to install on your managed devices or on the FortiManager system. For more information, see

Before you can use your FortiManager system as a private FDS, you must:

- Register your devices with Fortinet Technical Support and obtain 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 and FortiClient installations to the device list, or change the option to allow services to unregistered devices.

  For information about FDN service connection attempt handling or adding devices, see "Viewing FortiGuard services from devices and groups" on page 261 and "Managing Devices" on page 81. For more information about adding FortiClient installations, see "FortiClient Manager" on page 303.
- Enable and configure the FortiManager system's built-in FDS. For more information, see "Network interface" on page 59.

- Connect the FortiManager system to the FDN.

  The FortiManager system must retrieve packages from the FDN before it can redistribute them to devices on the device list. For more information, see “Connecting the built-in FDS to the FDN” on page 254.
- Configure each device or FortiClient installation 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 a device” on page 84.

This section contains the following topics:

Note: For news on current security threats, virus and spam sample submission, and FortiGuard service updates available through the FDN, including antivirus, IPS, web filtering and antispam, see the FortiGuard web site, http://www.fortiguardcenter.com/.

FortiGuard Center

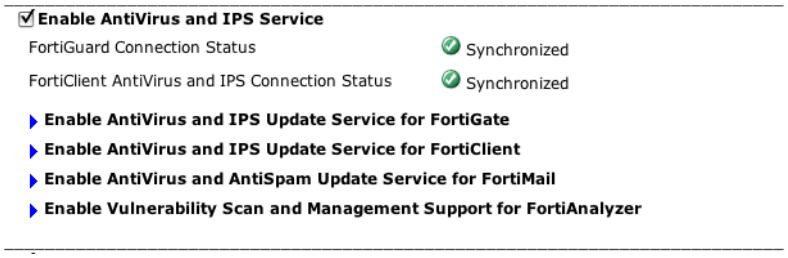
The FortiGuard Center, located in *System Settings* > *FortiGuard Center* in the root administrative domain, provides a central location for configuring and enabling your FortiManager system’s built-in FDS as an FDN override server.

By default, this option is disabled and devices contact FDN directly. After enabling and configuring FortiGuard, and your devices are configured to use the FortiManager system as their FortiGuard server, you can view overall and per device statistics on FortiGuard service benefits. For more information, see “Viewing FortiGuard services from devices and groups” on page 261.

The FortiGuard Center has four areas for configuration:

- IPS Update Service for FortiGate
- IPS Update Service for FortiClient
- AV and AS update Service for FortiMail
- Vuln Scan and Mgmt Support for FAL

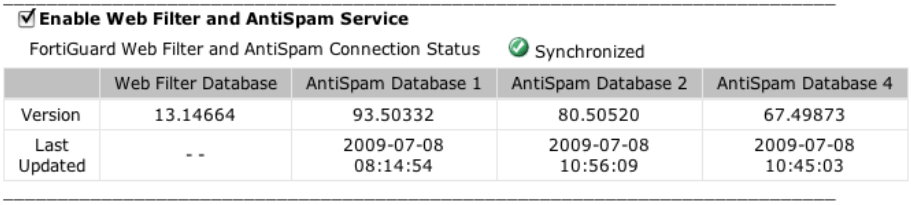
Figure 153: Enable FortiGuard settings



Enable Antivirus and IPS Service	When you select the check box beside *Enable Antivirus and IPS Service*, you are enabling FortiGuard antivirus and IPS services for FortiGate units. You will also be able to view the status of the antivirus and IPS connection for FortiClient.
FortiGuard Connection Status	The status of the current connection between the FDN and the FortiManager system. • **Disconnected** – A red down arrow appears when the FDN connection fails. • **Connected** – A green up arrow appears when the initial FDN connection succeeds, but a synchronization connection has not yet occurred. • **Out of Sync** – A gray X appears when the initial FDN connection succeeds, but the built-in FDS is disabled. • **Synchronized** – A green checkmark appears when the built-in FDS is enabled, and the FDN packages download successfully.
FortiClient AntiVirus and IPS Connection Status	The status of the current connection to the FDN for FortiClient antivirus and IPS services.
Enable AntiVirus and IPS Update Services for FortiGate/FortiClient /FortiMail/FortiAnalyzer	The current versions of engines and databases for antivirus and IPS services that are available on the FDS for the selected devices. You enable service updates by selecting the check boxes beside the OS firmware version number. If a check box is not selected, no databases or engines appear, only the OS firmware version number.

FortiGuard Web Filter and AntiSpam Service

Figure 154: Enable Web Filter and AntiSpam Service

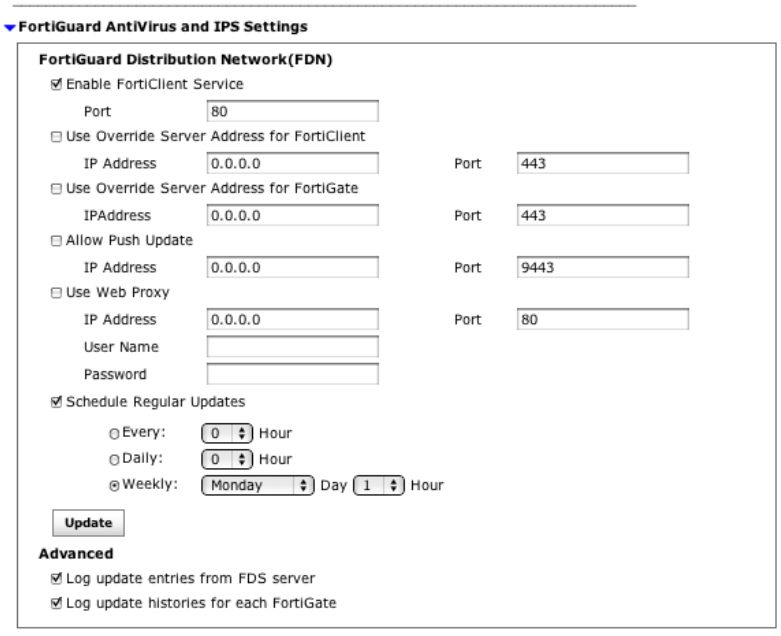


Enable Web Filter and AntiSpam Service	Select to enable FortiGuard web filtering and antispam services for all managed devices. This is available only when in EMS mode. The table displays when the databases are synchronized and their release version, and the date and time of the last update.
Version <database or engine version number>	The current version of the database or engine that was updated.

Enable Web Filter and AntiSpam Service	Select to enable FortiGuard web filtering and antispam services for all managed devices. This is available only when in EMS mode. The table displays when the databases are synchronized and their release version, and the date and time of the last update.
Version <database or engine version number>	The current version of the database or engine that was updated.
Enable Web Filter and AntiSpam Service	Select to enable FortiGuard web filtering and antispam services for all managed devices. This is available only in EMS mode. The table displays when the databases are synchronized and their release version, and the date and time of the last update.
Version <database or engine version number>	The current version of the database or engine that was updated.

FortiGuard Antivirus and IPS Settings

Figure 155: FortiGuard Antivirus and IPS Settings

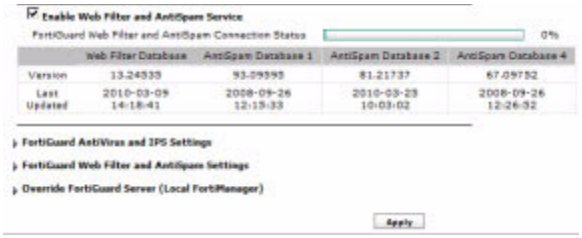


Enable FortiClient Service	Configure antivirus and IPS settings for FortiClients. Select to enable and if applicable, enter the port number that will be receiving FortiGuard service updates for FortiClient.
Use Override Server Address for FortiClient	Configure to override the default built-in FDS so that you can use a port or specific FDN server. To override the default server for updating FortiClient's FortiGuard services, see "Overriding default IP addresses and ports" on page 258.

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 updates through a web proxy" on page 257.
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 257.
Scheduled Regular Updates	Configure when packages are updated without manually initiating an update request. To schedule regular service updates, see "Scheduling updates" on page 259.
Update	Select to immediately update the configured antivirus and antispam settings.
Advanced	Enables logging of service updates and entries. If either check box is not selected, you will not be able to view these entries and events when you select View FDS and FortiGuard Download History.

FortiGuard Web Filter and Antispam Settings

Figure 156: FortiGuard Web Filter and Antispam Settings



Connection to FDS server(s)	Configure connections for overriding the default built-in FDS or web proxy server for web filter and antispam settings. To override an FDS server for web filter and antispam services, see "Overriding default IP addresses and ports" on page 258. To enable web filter and antispam service updates using a web proxy server, see "Enabling updates through a web proxy" on page 257.
Log Settings	Configure logging of FortiGuard web filtering and antispam events or configure access to • To configure logging of FortiGuard web filtering and antispam events, see "Logging FortiGuard Web Filtering or Antispam events" on page 267
Override FortiGuard Server (Local FortiManager)	Configure and enable alternate FortiManager FDS devices, rather than using the local (current) FortiManager system. You can set up as many alternate FDS locations, and select what services are used. To configure access to public web filtering and antispam servers, see "Accessing public FortiGuard web filtering and antispam servers" on page 259
View FDS and FortiGuard Download History	View the types of FortiGuard services that occurred, such as poll and push updates, from FDS, FortiGuard or FortiClient.

Additional number of private FortiGuard servers (excluding this one) (1) +	Select the + icon to add a private FortiGuard server. When adding a private server, you must enter its IP address and time zone. Private FortiGuard servers are used for
Enable AntiVirus and IPS Update Service for Private Server	When one or more private FortiGuard servers are configured, update AntiVirus and IPS through this private server instead of using the default FDN. This option is available only when a private server has been configured.
Enable Web Filter and AntiSpam Update Service for Private Server	When one or more private FortiGuard servers are configured, update the Web Filter and AntiSpam through this private server isntead 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.

Note: The FortiManager system's network interface settings can restrict which network interfaces provide FDN services. For more information, see "Network interface" on page 59.

Connecting the built-in FDS to the FDN

When you enable the built-in FDS, and initiate an update either manually or by 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 *System Settings* > *FortiGuard Center* > *Configuration*.

2 Enable the types of FDN services that you want to provide through your FortiManager system's built-in FDS.

The types of FDN services also include Vulnerability Scan and Management Support for managed FortiAnalyzer units. For more information, see "Configuring FortiGuard services in the FortiGuard Center" on page 256.

3 Select *Apply*.

The built-in FDS attempts to connect to the FDN. To see the connection status go to *System Settings* > *FortiGuard Center*.

Disconnected	A red down arrow appears when the FDN connection fails.
Connected	A green up arrow appears when the initial FDN connection succeeds, but a synchronization connection has not yet occurred.

Out Of Sync	A gray X appears when the initial FDN connection succeeds, but the built-in FDS is disabled, and so cannot synchronize.
Synchronized	A green checkmark appears when the built-in FDS is enabled, and FDN package downloads were successfully completed.

If the built-in FDS cannot connect, you may also need to enable the selected services on a network interface. For more information, see "Network interface" on page 59.

Note: If you still cannot connect to the FDN, check routability, 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, "FDN port numbers and protocols" on page 258 and the Knowledge Center article Fortinet Distribution Network: Accessing and Debugging FortiGuard Services.

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. For more information, see "Viewing FortiGuard services from devices and groups" on page 261.

Procedures for configuring devices to use the built-in FDS vary by their device type. See the documentation for your device for information.

Note: 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 settings" on page 59.

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 4.0 and higher, but the FortiManager system's built-in FDS listens for those requests on TCP 8890. In this case, the FortiGate unit's update requests would fail until you configure the unit to send requests on TCP 8890.

In some cases, the device may not be configurable; instead, you must configure the FortiManager system to listen on an alternate port. For example, FortiClient 2.0 or earlier requires TCP 80 for service requests, and is not configurable. In this case, configure the built-in FDS to listen for FortiClient requests on TCP 80.

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 *Unregistered Device Options* 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 web-based manager), 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 as configured in Unregistered Device Options.

Note: Unregistered FortiClient connections are handled in FortiClient Manager.

To configure connection attempt handling

1 Go to *Device Manager* > *Unregistered Device* > *Unregistered Device Options*.

2 Select which action the FortiManager system performs when receiving a connection attempt from an unregistered device:

- Add unregistered devices to device table, but ignore service requests

  The device appears in the Unregistered Devices item in the device list, but its connection attempt is otherwise ignored.

- Add unregistered devices to device table, and allow FortiGuard service and central management service.

  The device appears in the Unregistered Devices item in the device list, and will be allowed to receive FortiGuard services.

3 Select *Apply*.

Configuring FortiGuard services in the FortiGuard Center

The FortiGuard Center 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 this 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 257.

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, enter 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.

Note: The built-in FDS may not receive push updates if the external IP address of any intermediary NAT device is dynamic (such as an IP address from PPPoE or DHCP). When the NAT device's external IP address changes, the FortiManager system's push IP address configuration becomes out-of-date.

To enable push updates to the FortiManager system

1 Go to *System Settings* > *FortiGuard Center* > *Configuration*.

2 Select the arrow to expand the *FortiGuard AntiVirus and IPS Settings*.

3 Select the check box 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, enter 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 Select *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.

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 *System Settings* > *FortiGuard Center* > *Configuration*.

2 If configuring a web proxy server to enable web filtering and antispam updates, expand *FortiGuard Web Filter and AntiSpam Settings.*

3 If configuring a web proxy to enable antivirus and IPS updates, expand *FortiGuard AntiVirus and IPS Settings*.

4 Select the check box 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 Select *Apply*.

7 Select *Update* to immediately connect and receive updates from the FDN.

The FortiManager system connects to the override server and receives updates from the FDN.

If the FDN connection status is Disconnected, the FortiManager system cannot connect through the web proxy.

Overriding default IP addresses and ports

FortiManager systems' built-in FDS connect 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 *System Settings* > *FortiGuard Center* > *Configuration*.

2 If you want to override the default IP address or port for synchronizing with available FortiGuard Antivirus and IPS updates, select the arrow to expand *FortiGuard AntiVirus and IPS Settings*.

- Select the check box beside *Use Override Server Address for FortiGate* and enter the IP address and/or port number for all FortiGate units.
- Select the check box beside *Use Override Server Address for FortiClient* and enter the IP address and/or port number for all FortiClients.

3 If you want to override the FortiManager system's default IP address or port for synchronizing with available FortiGuard Antispam and Web Filtering updates, select the arrow to expand *FortiGuard Web Filter and AntiSpam Settings*.

Select the check box beside *Enable Server Override* and enter the IP address and/or port number.

4 Select *Apply*.

5 Select *Update* to immediately connect and receive updates from the FDN.

The FortiManager system connects to the override server and receives updates from the FDN.

If the FDN connection status remains disconnected, the FortiManager system cannot 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.

For troubleshooting information and details on FDN ports, see and the Knowledge Center article FDN Services and Ports.

After connecting to the FDS, you can verify connection status on the FortiGuard Center page. For more information about connection status, see "Connecting the built-in FDS to the FDN" on page 254.

Scheduling updates

Keeping the built-in FDS up-to-date is important to provide current 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. As well, you never need to worry about remembering when, or if you did, update the database definitions.

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 *System Settings* > *FortiGuard Center* > *Configuration*.
2 Select the arrow to expand *FortiGuard AntiVirus and IPS Settings*.
3 Select the check box beside *Schedule Regular Updates*.
4 Specify an hourly, daily, or weekly schedule.
5 Select *Apply*.

To schedule web filtering and antispam polling

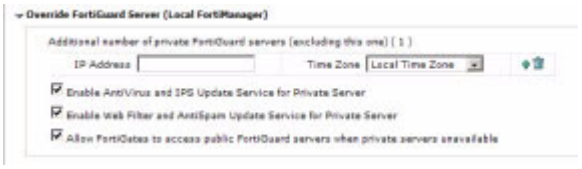
1 Go to *System Settings* > *FortiGuard Center* > *Configuration*.
2 Select the arrow to expand *FortiGuard Web Filter and AntiSpam Settings*.
3 In *Polling Frequency*, select the number of hours and minutes of the polling interval.
4 Select *Apply*.

Note: If you have formatted your FortiManager system's hard disk, polling and lookups will fail until you restore the URL and antispam databases. For more information, see "Restoring the URL or antispam database" on page 268.

Accessing public FortiGuard web filtering and antispam servers

You can configure the FortiManager system to allow the managed FortiGate units to access public FortiGuard web filter or antispam servers in the event local FortiGuard web filter or antispam server URL lookups fail. You can specify up to two private servers (which includes the current one) where the FortiGate units can send URL queries.

Figure 157: Overriding FortiGuard Server



Note: Access to public servers is available only on the FortiManager-3000 unit when in root ADOM in EMS mode.

To access public FortiGuard web filter and antispam servers

1. Go to *System Settings* > *FortiGuard Center* > *Configuration*.
2. Expand *Override FortiGuard Server (Local FortiManager)*.
3. Select the *Plus* sign next to *Additional number of private FortiGuard servers (excluding this one)*.
4. Enter 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.
   - Check the *Enable AntiVirus and IPS update Service for Private Server* if you want the FDS updates to come from a private server.
   - Check the *Enable Web Filter and AntiSpam Update Service for Private Server* if you want the updates to come from a private server.
   - Click *Allow FortiGates to access public FortiGuard servers when private servers unavailable* if you want to the updates to come from public servers in case the private servers are unavailable.
7. Select *Apply*.

Manually uploading antivirus and IPS updates

The built-in FDS will retrieve antivirus and IPS update packages from the FDN automatically at the scheduled time, then re-distribute them to requesting devices; however, you can also manually upload the antivirus and IPS packages to the FortiManager system, and manually re-distribute them to devices.

- You can retrieve antivirus and IPS update packages from the support web site to your computer, then upload them to the FortiManager system. This can be useful if your FortiManager system must distribute packages other than the ones currently available from the FDN. (In this case, you would also disable synchronization with the FDN.)
- You can manually distribute update packages to devices from the FortiManager system. This can be useful when the antivirus and IPS packages are reverted, which can occur when restoring device firmware.

Uploads to devices can be initiated by either push or traditional upload methods. Both methods require you to enable SSH and HTTPS administrative connections from the FortiManager system's IP address on the device's network interface. Push additionally requires that the device be enabled to receive push messages.

To manually upload antivirus or IPS updates to one or more devices

1. Select a device in the device manager.
2. Select *Relay Service*.
3. Scroll to the bottom of the page and select *Manual Update*.
4. Select *Transfer* for the package that you want to upload.
5. Select the recipient devices from the list of available devices, then select the right arrow to move them to the *Transfer To* list.
6. Select *OK*.

   The FortiManager system uploads the selected package to the selected device(s).

To push antivirus or IPS updates to one or more devices

1 Select a device in the device manager.

2 Select *Relay Service*.

3 In the *License Information* area, select *Push* for the device that you want to update.

A UDP message announcing the availability of the most current update is sent to the device. If the device is enabled to receive push updates, it then downloads the update from the FortiManager system.

Note: Manual uploads do not bypass the requirement that the FortiManager system must be able to connect to the FDN to validate device licenses for FortiGuard Antivirus and IPS.

Viewing FortiGuard services from devices and groups

The Device Manager can be used to display FortiGuard license information and threat detection statistics for devices that use the FortiManager unit for FortiGuard service updates and queries. You can also push or manually issue FortiGuard service updates to devices registered with Device Manager.

FortiGuard service statistics for an individual device or group are not available until you:

- enable FortiGuard services via the built-in FDS (see “Connecting the built-in FDS to the FDN” on page 254)
- enable FortiGuard service logging (see “Logging events related to FortiGuard services” on page 266)
- register and connect the device/group to Device Manager
- provide the device/group with valid FortiGuard service licenses
- configure the device/group to request FortiGuard updates and ratings from the FortiManager system, instead of the public FDN

Statistic columns are sortable. For example, you could sort device names in ascending order (from A to Z), or IP addresses in descending order (from high to low numbers).

To sort columns in ascending or descending order, select the column heading. Each time you click the column heading, the column will cycle between ascending and descending order. An arrow next to the column heading indicates the current sort order: an up arrow indicates ascending order, and a down arrow indicates descending order. By default, columns are in ascending order.

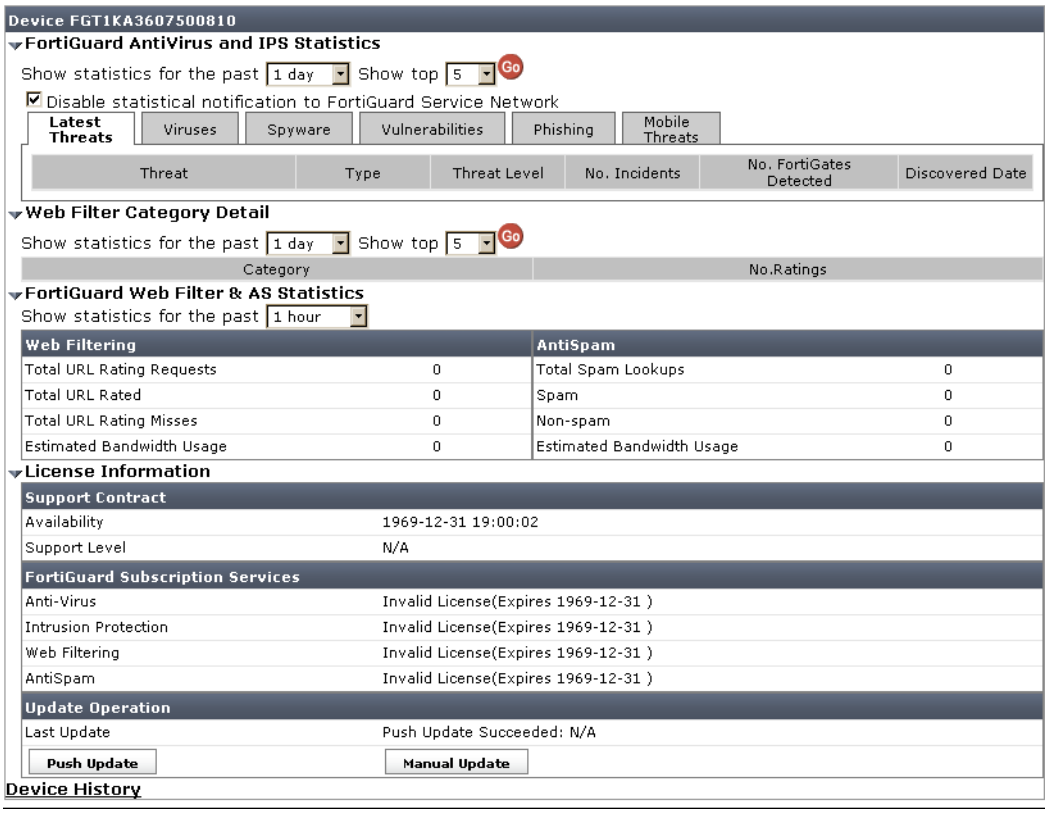
To view a device’s FortiGuard service usage statistics

1 From the Device Manager select a device.

2 Select *Relay Service*.

Note: Statistics are not available for unregistered devices. Additionally, the FortiManager system cannot send Manual Update or Push messages to unregistered devices.

Figure 158: Service Usage for an individual device

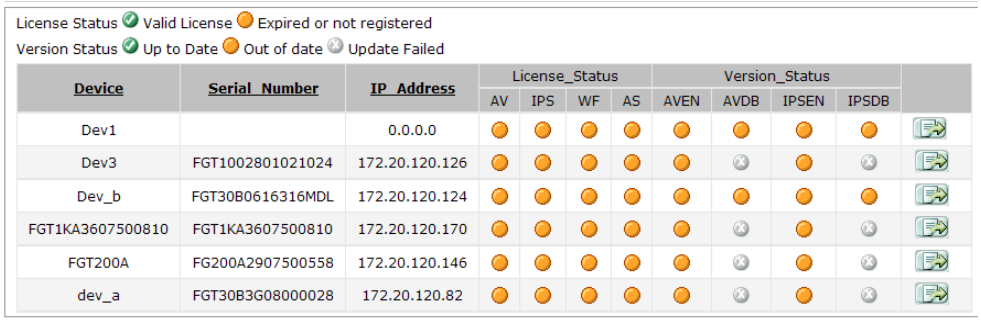


To view device group's FortiGuard service usage statistics

1 From the Device Manager select a device group.

2 Select *Service Usage*.

Figure 159: Service Usage for a device group



FortiGuard antivirus and IPS Statistics for a device

If antivirus and IPS updates from the built-in FDS are currently disabled, a warning message about the service being disabled appears:

To view FortiGuard antivirus and IPS statistics for a device, in the device manager select a device and select *Relay Service*. Then select the arrow to expand *FortiGuard AntiVirus and IPS Statistics*.

Figure 160: Service Usage: FortiGuard AV and IPS Statistics

Show statistics for the past *n*	Select a number of days (up to 7) to view statistics for that period of time and then select *Go*.
Show top *n*	Select a number to view the top threat types and then select *Go*.
Disable statistical notification to FortiGuard Service Network	Select if you do not want FortiManager system to send statistical information on threats to Fortinet. By default, this feature is enabled.
Latest Threats, Viruses, Spyware, Vulnerabilities, Phishing, Mobile Threats	Select a tab to view detailed information about the latest threats, viruses etc. detected on the selected FortiGate device.
Threat, Virus, spyware, Vulnerability, Phishing, Mobile Threat	The name of the threat, virus etc.
Type	The category of threat, such as a Mass-Mailer.
Threat Level	The severity level of the threat (virus etc.): the higher the severity, the higher the threat level.
%	The threat level as a percent.
No. Incidents	The number of times that the threat was detected.
No. FortiGates Detected	The number of FortiGate devices that detected the threat.
Discovered Date	The date that Fortinet added the ability to recognize the threat, such as an IPS signature, virus signature, etc.

Web Filter Category Detail

Web Filter Category Detail displays FortiGuard Web Filtering category and rating statistics, and is available on FortiManager-3000 models and greater.

To view web filtering category details for a device, in the device manager select a device and select *Relay Service*. Then select the arrow to expand *Web Filter Category Detail*.

Figure 161: Service Usage: Web Filter Category Detail

FortiGuard Web Filter and Antispam Statistics

Web and spam filtering statistics track the number of rating queries and their associated bandwidth, and are available on FortiManager-3000 models and greater.

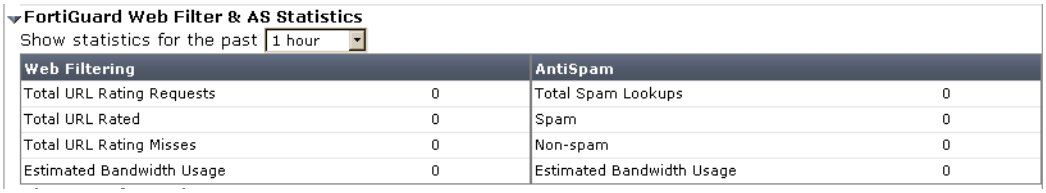
Statistics are either a group total, or only for the device, depending on whether you have selected a single device or a group in the Navigation Pane.

If web filtering and antispam lookups from the built-in FDS are currently disabled, the following message appears:

```
Warning: This Update Manager service is currently disabled
```

To view FortiGuard Web Filtering and Antispam statistics for a device, in the device manager select a device and select *Relay Service*. Then select the arrow to expand *FortiGuard Web Filter & AS Statistics*.

Figure 162: Service Usage: FortiGuard Web Filter & AS Statistics



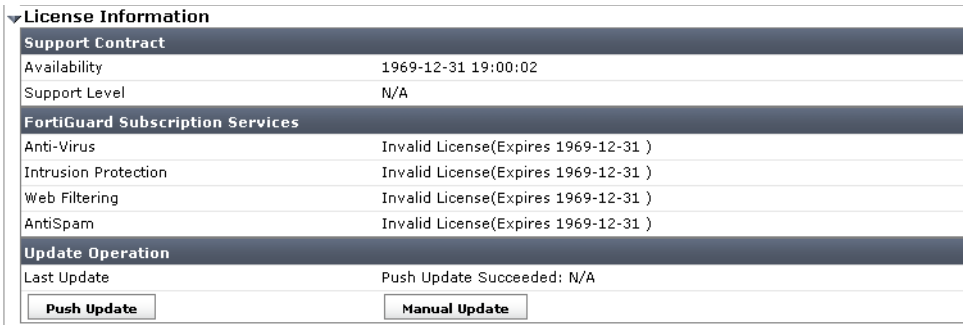
License Information

License information includes devices' FortiGuard service licenses, support contracts and update status. Statistics are either a group total, or only for the device, depending on whether you have selected a single device or a group in the Navigation Pane.

Single device license information

To view license information for a device, in the device manager select a device and select *Relay Service*. Then select the arrow to expand *License Information*.

Figure 163: Service Usage: License Information (single device)

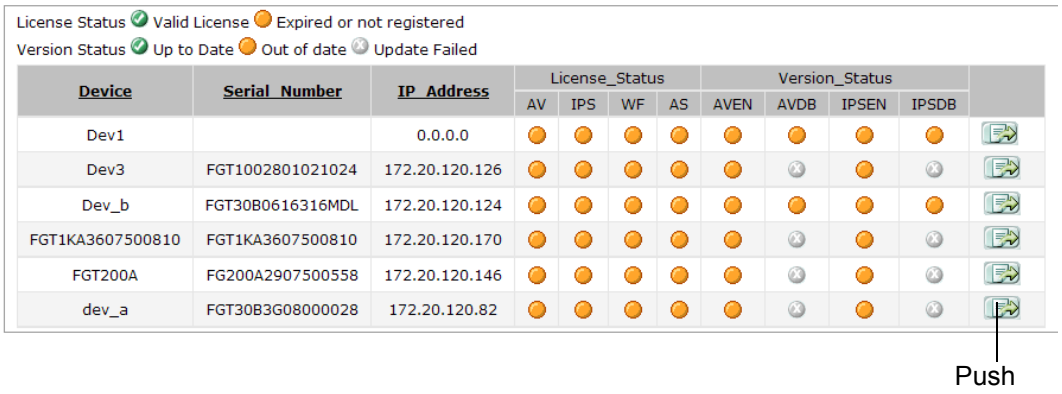


Support Contract	Information about the device's support contract.
Availability	The date on which the support contract became valid.
Support Level	The level of support that Fortinet provides for the device.
FortiGuard Subscription Services	
Anti-Virus	The status of the FortiGuard subscription for antivirus.
Intrusion Protection	The status of the FortiGuard subscription for Intrusion Protection and application control.
Web Filtering	The status of the FortiGuard subscription for web filtering.
AntiSpam	The status of the FortiGuard subscription for antispam.
Update Operation	
Last Update	The last update that was attempted (push update or scheduled update) and whether the update succeeded or failed.
Push Update	If push updates are enabled an configured for the FortiGate device, select Push to send an update availability notification to the FortiGate device. For more information about enabling and configuring push updates, see "Connecting the built-in FDS to the FDN" on page 254.
Manual Update	Select to manually update antivirus and IPS signatures by selecting antivirus and IPS signature files stored on the FortiManager device and selecting *Push*.

Device group license information

To view license information for a device group, select a device group and select *Service Usage* for that device group.

Figure 164: Device group Service Usage: License Information



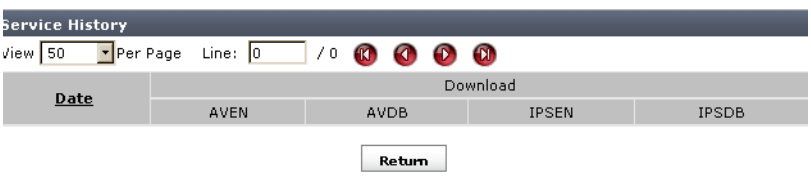
Device, Serial Number, IP address	Identifying information for the devices in the device group. You can sort the information in the table by selecting these column headings.
License Status	Displays the license status for antivirus (AV), intrusion protection (IPS), web filtering (WF), and antispam (AS) and firmware manager (FWM). The status of each license is displayed using the icons described at the top of the web-based manager page: • Valid License - This license is valid and up-to-date. • Expired or not registered - This license is not valid. It is either expired and requires renewing, or has not been registered yet. • Unknown - The status of this license can not be determined. Check the device for more information.
Version Status	Displays the version status for antivirus engine, antivirus database, IPS engine, and IPS database. The status of each license can be one of: • Up to date - This version is the most recent available version. • Out of date - This version can be updated to a newer version. • Unknown - This version can not be determined. Check the device for more information.
Push icon	Select to start a push update on this device. A message will be displayed with the device, action taken, and the result.

Device History

Device History (also called Service History) provides historical data on what services have been uploaded successfully to the device.

To view device history for a device, in the device manager select a device and select *Relay Service*. Then scroll to the bottom of the page and select *Device History*.

Figure 165: Device History



View *n* Per Page	The number of lines you are currently viewing on the page. Select 50, 100, 200 or 500 lines.
Line *n* / *n*	The current line you are viewing out of the total number of lines, for example, line 2 of 50. Enter a number to go to a specific line, for example, 5 to view line 5 in the list. Use the arrows to go to the previous page, next page, first page, or last page.
Date	The date the last update occurred. You can display dates in either ascending order or descending order by selecting the Date column heading.
Download	The antivirus and IPS versions that were downloaded to that device.
AVEN	Whether the antivirus engine is up to date, out of date, or if the last update failed.
AVDB	Whether the antivirus database is up to date, out of date, or if the last update failed.
IPSEN	Whether the IPS engine is up to date, out of date, or if the last update failed.
IPSDB	Whether the IPS database is up to date, out of date, or if the last update failed.

Logging events related to FortiGuard services

You can log a variety of events related to FortiGuard services. Depending on your logging selections and which aspect you want to view, you may be able to view these events from these locations:

- from *System Settings* > *Local Log* > *Log Access*
- from *System Settings* > *FortiGuard Center* > *Log* > *Update Log*
- from *System Settings* > *FortiGuard Center* > *Log* > *Download History*

Note: Logging events from the FortiManager system's built-in FDS requires that you also enable local event logging. For instructions on enabling local event logging, see "Local log settings" on page 71.

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 *System Settings* > *FortiGuard Center* > *Configuration*.
2. Select the arrow to expand *FortiGuard AntiVirus and IPS Settings*.
3. Enable *Log update entries from FDS server*.
4. Select *Apply*.

To log updates to FortiGate devices

1. Go to *System Settings* > *FortiGuard Center* > *Configuration*.
2. Select the arrow to expand *FortiGuard AntiVirus and IPS Settings*.
3. Enable *Log update histories for each FortiGate unit*.
4. Select *Apply*.

Logging FortiGuard Web Filtering or Antispam events

You can track FortiGuard Web Filtering and Antispam 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 Antispam events.

To log rating queries

1 Go to *System Settings* > *FortiGuard Center* > *Configuration*.

2 Select the arrow to expand *FortiGuard Web Filtering and AntiSpam Settings*.

3 Select the log settings:

FortiGuard Web Filtering	
Log URL rating misses	Logs URLs without ratings.
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 all Spam lookups	Logs all spam lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
Log non-spam events	Logs email rated as non-spam.

4 Select *Apply*.

Viewing service update log events

You can view the logged service update events from either the FortiGuard Center or from a device or device group.

To view updates to registered FortiGate devices which use the FortiManager system's FDS, select a device from the device manager, select *Relay Service*, and select *Device History*.

To view update logs for the built-in FDS

1 Go to *System Settings* > *FortiGuard Center* > *Log* > *Download History*.

2 From the *Service* list, select either *FDS*, *FGD* or *FCT*.

- FDS: Packages that the FortiManager system can redistribute to FortiGate units, for their local use.
- FCT: Packages that the FortiManager system can redistribute to FortiClient installations.
- FGD: Packages that the FortiManager system uses to respond to queries, such as URL rating queries, from FortiGate units.

Service indicates the category of packages downloaded by the FortiManager system.

3 From the *Event* list, select one of the following: *All Event* to view all events, *Push Update*, *Poll Update*, or *Manual Update*.

Event indicates the update mechanism, such as updates that occur by either push or poll mechanisms.

4 Select *Go*.

Details of the selected update events appear:

Date	The date and the time of the update or license check.
Event	The type of the update event, such as Poll Update or Push Update.

Status	The results of the update connection, such as Success, Up to Date, or Connection Failed.
Download	The version number for each item that the built-in FDS can download from the FDN. Download types vary by your selected Service. These appear if Service is FDS: • AVEN: FortiGuard Antivirus engine • AVDB: FortiGuard Antivirus signature database • IPSEN: FortiGuard IPS engine • IPSDB: FortiGuard IPS signature database • FASE: FortiGuard Antispam engine • FASR: FortiGuard Antispam rating • FEEN: FortiMail antispam engine • FEDB: FortiMail antispam database These appear if Service is FGD: • SPAM001: FortiGuard Antispam URI database • SPAM002: FortiGuard Antispam IP address database • SPAM004: FortiGuard Antispam hash database • FURL: FortiGuard Web Filtering URL database • FGAV: FortiGuard Antivirus query database These appear if Service is FCT. • FVEN: FortiGuard Antivirus engine for FortiClient • FVDB: FortiGuard Antivirus signature database for FortiClient • FSEN: FortiGuard Antivirus engine for FortiClient Mobile Symbian • FSDB: FortiGuard Antivirus signature database for FortiClient Mobile Symbian • FMEN: FortiGuard Antivirus engine for FortiClient Windows Mobile • FMDB: FortiGuard Antivirus signature database for FortiClient Windows Mobile A green check mark appears next to all version numbers if one or more of the packages was updated during that connection (that is, the Status column is *Success*). A gray X appears next to all version numbers if none of the packages were updated during that connection (that is, the Status column is *Up to Date* or *Connection Failed*).

To view update logs from FortiGate devices

1. Select a device in the device manager.
2. Select *Relay Service*.
3. Select *Device History*.

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 Antispam 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).

Changing Firmware

Instead of upgrading or downgrading each managed device manually, you can change device firmware through your FortiManager unit.

FortiManager units can store and install FortiGate, FortiAnalyzer and FortiManager firmware images. FortiManager units can receive local copies of firmware images by either downloading these images from the Fortinet Distribution Network (FDN) or by accepting firmware images that you upload from your management computer.

If you are using the FortiManager unit to download firmware images from the FDN, FortiManager units first validate device licenses, including each member of high availability (HA) clusters. The FDN validates support contracts and provides a list of currently available firmware images. For devices with valid Fortinet Technical Support contracts, you can download new firmware images from the FDN, including release notes.

After firmware images have been either downloaded from the FDN or imported to the firmware list, you can either schedule or immediately upgrade/downgrade a device or group's firmware.

Firmware versions and maintenance releases do not always contain the same configuration options and because these options are different, you may need to configure the device or group and resync its configuration after changing a device or group's firmware.

This section contains the following topics:

Note: For more information about backing up firmware, upgrading firmware, including general upgrading information, see "Managing Firmware Versions" on page 393.

Viewing a device or group's firmware

You can view a device or group's currently installed firmware, as well as historical changes of firmware images. You can use this information to determine which devices you may want to upgrade.

In *Device Manager*, the Summary tab displays the firmware version number of the currently installed firmware for an individual device or group. The Firmware tab, located after selecting a device, displays detailed firmware information for an individual device or group, including the currently installed firmware image, scheduled firmware changes, and the history of past firmware changes.

When viewing a device or group's firmware information, you can also schedule a future or immediate firmware change, or clear all future scheduled changes. For more information, see "Installing firmware images" on page 276.

Figure 166: Firmware Information (device)

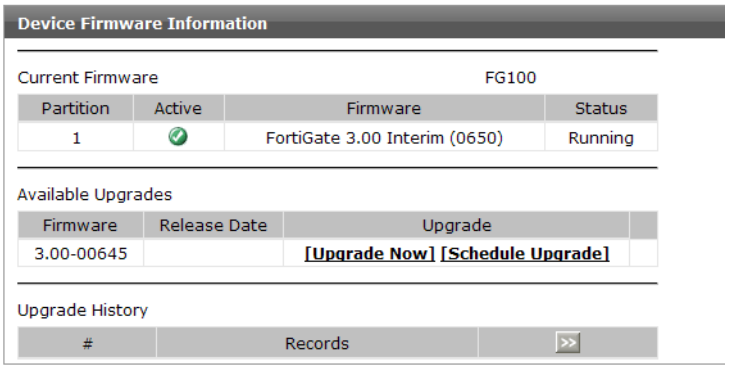
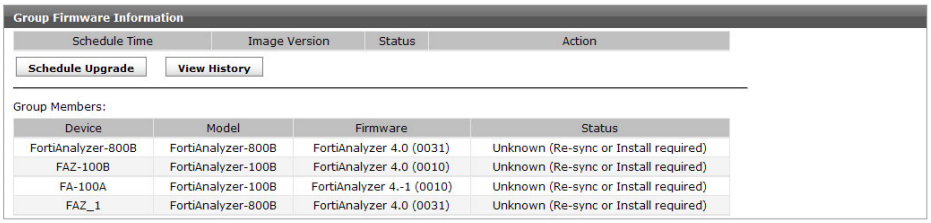


Figure 167: Firmware Information (group)



Schedule Time	The time when the next firmware change is scheduled to begin. Firmware changes can be scheduled at either the individual device or group level. For more information, see "" on page 276.
Image Version	The firmware version that the device will have when the scheduled firmware change is complete.
Status	The the upgrade status on the device, such as *None* (if no upgrade is currently scheduled), or *Accepted* (if an upgrade is scheduled, but not yet in progress).
Delete icon	Select to cancel the next scheduled firmware change. This appears only when firmware information displays.
Schedule Upgrade	Select to schedule an immediate or future upgrade for the device.
View History	Select to view a detailed audit trail of all firmware upgrades the device has received from the FortiManager.
Group Members	The firmware version and configuration synchronization information for each device in the group. This does not appear when an individual device is currently selected.
Device	The device's host name.
Model	The device's model.
Firmware	The firmware version currently running on the device.
Status	The configuration synchronization status of the device with the FortiManager unit. If the status is not *Synchronized*, you might need to retrieve or deploy the device's configuration to synchronize the configuration copy stored on the device itself with the local configuration copy stored on the FortiManager unit. For more information about synchronization, see "Checking device configuration status" on page 277.

To view a device or group's firmware details

1 Go to *Device Manager* and select the type of device you want to view. For example, if you have at least one FortiGate unit registered, *FortiGate* will appear as an option.

If you want to view a group's firmware details, go to *Device Manager* > *Group*.

2 Select a unit name to view the unit details.

If want to view the details of a group, select a group name.

3 Select the *Firmware* option in the *Device Manager* list.

The firmware version and any scheduled upgrades for the selected device or group are listed.

If a group is currently selected, collective information is listed, such VDOM status, description, and NAT or transparent operation mode. Information for each device in the group is also listed, so that you can quickly verify devices whose firmware version is different from the group.

To view a device or group's firmware history

1 Go to *Device Manager* and select the type of device you want to view. For example, if you have at least one FortiGate unit registered, *FortiGate* will appear as an option.

If you want to view a group's firmware details, go to *Device Manager* > *Group*.

2 Select a unit name to view the unit details.

If want to view the details of a group, select a group name.

3 Select the *Firmware* option in the *Device Manager* list.

4 To view all of a device's firmware history, select the *All History* icon in *Upgrade History.*

5 To view all of a group's firmware history, select *View History* and then select *All*.

6 To view a specific time period of a group's firmware history, select *View History*, select *Select*, and then configure the start and end times.

7 Select *OK*.

8 To return to the previous page after viewing either a device or group's firmware history, select *Return*.

The group or device's firmware version and any scheduled upgrades appear.

If a group is currently selected, collective information is listed, such VDOM status, description, and NAT or transparent operation mode. Information for each device in the group is also listed, so that you can quickly verify devices whose firmware version is different from the group.

Note: If the options *Schedule Upgrade* and *Delete* are grayed out, device locking is enabled. Before you can make any configuration changes to a device, you should lock the device to avoid configuration conflicts with other administrators. For more information on device locks, see "Device configuration locks" on page 69

To determine if a FortiGate device or group has an available firmware upgrade

1 Go to *System Settings* > *Firmware Images*.

2 Expand a device type to reveal the available firmware versions, maintenance releases and patch releases.

3 Compare the firmware image to the current firmware image on the FortiGate device or group.

You must have root administrative privileges to access *System Settings* > *Firmware Images*.

For more information about downloading firmware images, see “Downloading firmware images” on page 274. For information about how to schedule or immediately install a firmware upgrade for a device or group, see “Installing firmware images” on page 276.

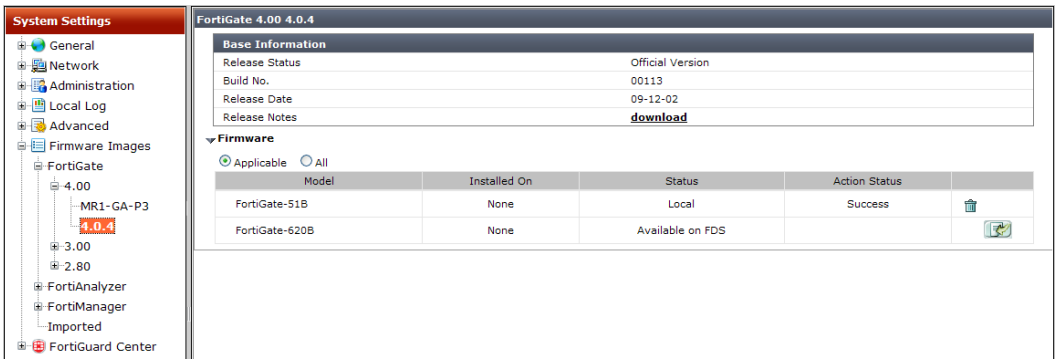
Downloading firmware images

You must first download a local copy of the firmware image to the FortiManager unit to use the FortiManager unit to change managed FortiGate devices’ firmware, or to change the FortiManager unit’s own firmware.

The Firmware Images page, located in *System Settings*, displays all firmware images uploaded to the FortiManager unit from your computer. If a connection to the FDN is available, Firmware Images also displays official FDN releases that you can download to the FortiManager unit. These local copies of firmware images stored on the FortiManager unit are available for use when scheduling firmware changes for FortiGate units, or when changing the firmware of the FortiManager unit itself.

To display all firmware images stored on the FortiManager unit, or to download a local copy of a firmware image, go to *System Settings* > *Firmware Images*.

Figure 168: Firmware Images



Base Information	
Release Status	The release status of the firmware image.
Build No.	The build number of the firmware image, which can be used to distinguish different images with the same major release version.
Release Date	The release date of the firmware image.
Release Notes	Select to download the release notes for the firmware image.
Firmware	
Applicable	Select to display only the devices that the specific firmware is for.
All	Select to display all available firmware for all of the devices.
Model	The firmware image’s compatible device model.
Installed On	Devices on which the FortiManager unit has installed with that firmware image.
Status	Whether the firmware has been downloaded to the FortiManager unit (*Local*) or is merely available on the FDN (*Available on FDS*).
Action Status	Whether the firmware is pending download (*Accept*) or has completed the download (*Success*).

Delete icon	Delete to local copy of a downloaded firmware image. If a firmware image is deleted, it can be downloaded again.
Download icon	Download a local copy of the firmware image from the FDN. For more information, see "To retrieve an image from the FDN to the FortiManager unit" on page 275.

To retrieve an image from the FDN to the FortiManager unit

1 Go to *System Settings* > *Firmware Images*.

2 Expand the device type and the firmware version to reveal the available firmware images, and select one of the images.

If no FDN releases appear in the Navigation Pane, check the unit's FDN connection. For more information, see "Connecting the built-in FDS to the FDN" on page 254.

3 Select *Applicable* if you want to display firmware that is applicable to certain devices. Select *All* if you want to display all available firmware for all devices.

4 In the column corresponding to the device's Model, select *Download*.

If attempts to download the firmware image fail with the error message, "This image is not downloadable," verify that you have registered devices of that model with Fortinet Technical Support. Images cannot be downloaded unless at least one device of that model has been registered with Fortinet, and has a valid support contract. If these requirements are satisfied, but the error message still appears, wait ten minutes to allow the FortiManager unit to validate device support contracts with the FDN, then retry the download.

To view support contract status and expiration date, in the Device Manager, select the device, then select the *Summary* tab. Support contract information is located in the License Information area.

Download time varies by your connection speed and the size of the file. The Status and Action Status columns indicate if the firmware image is available, if its download to the FortiManager unit is in progress, or if the download has successfully completed.

Table 12: Download progress indicators in Firmware Images

Status	Action Status	Indication
Available on FDS		The firmware image is available on the FDN, but the FortiManager unit has no local copy.
Available on FDS	Accept	The FortiManager unit is currently downloading a local copy of the firmware image.
Local	Success	The FortiManager unit has successfully downloaded a local copy of the firmware image.

To import a firmware image that you have already downloaded to your computer

1 Go to *System Settings* > *Firmware Images*.

2 Select *Imported*.

3 Select *Create New*.

4 Select *Browse* to locate the file.

5 Select *OK*.

Upload time varies by your connection speed and the size of the file.

To delete a local copy of a firmware image

1 Go to *System Settings* > *Firmware Images*.

2 Select *Imported*.

3 In the *Imported Firmware Images* list, in the row corresponding to the firmware image that you want to delete, select *Delete*.

A confirmation message appears.

4 Select *OK*.

Installing firmware images

When you are ready to install a firmware image, use the procedures in "Managing Firmware Versions" on page 393. This section provides detailed instructions on how to properly install firmware images to your FortiManager unit and managed devices, including how to test the firmware image before permanently installing it on your FortiManager unit. You can also use the procedures in "Firmware Update" on page 50; however, Fortinet recommends using the procedures in "Managing Firmware Versions" on page 393 because of its detailed instructions on how to properly install firmware images, which helps you to successfully upgrade the device or FortiManager unit.

You can install firmware images that are either official FDN release images or imported images. When installing a firmware image, you can have the firmware image installed on a specific day and during a specific period of time. For example, you might update firmware during the night when there is less traffic on your network. If you have scheduled a firmware upgrade, you can cancel it.

You cannot cancel firmware changes that:

- have already been attempted at least once, and are configured to retry *n* times
- are currently in progress.

You can immediately change a FortiGate device or group's firmware, or you can schedule a change in the future.

Note: If the FortiManager unit's support contract is invalid or expired, a firmware update can appear to be available from the FDN in *System Settings* > *Firmware Images*. Renew your Fortinet Technical Support contract if, when you select *Download*, a message states that you need to renew the FortiManager unit's support contract.

Installing 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.

For more information on the configuration and installation workflow, see "Configuration and installation workflow" on page 18.

This section contains the following topics:

Checking device configuration status

In the *Device Manager* window, when you select *All FortiGate*, *All FortiAnalyzer*, *All FortiMail, All FortiSwitch,* or *All FortiCarrier* in the device tree, you can view a device's basic information under the *Summary* tab. 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 resynchronize 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 FortiAnalyzer unit, FortiCarrier, or FortiMail unit.

Note: If you see padlock icons beside the devices in the Navigation Pane, it means that device locking is enabled. Before you can make any configuration changes to a device, you must lock the device to avoid configuration conflicts with other administrators. For more information on device locks see "Device configuration locks" on page 69.

To check the status of a configuration installation on a FortiGate unit

1. Go to *Device Manager* > *FortiGate*.
2. On the All FortiGate page, select the FortiGate unit that you want to check the configuration status of.

   You are automatically redirected to *System* > *Status* > *Status* of that unit.
3. On the Status page, locate the Configuration and Installation Status widget.
4. Verify the status in the *Configuration Change Status* row.

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

To view the device installation history on a FortiGate unit

1. In the left pane, select the Revision menu.

2 Select *View Installation History*.

You are automatically redirected to the View Installation History page.

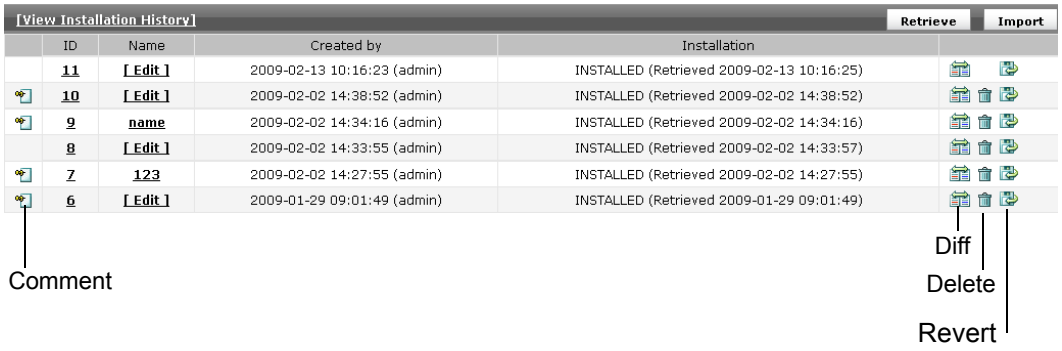
Managing configuration revision history

In the *Device Manager* window, select a device in the device tree and then select the *Revision History* tab to view the FortiManager repository.

Note: If you see padlock icons beside the devices in the Navigation Pane, it means that device locking is enabled. Before you can display all functionalities under the configuration repository, you must lock the device. You also need to do so before you can make any configuration changes to a device in order to avoid configuration conflicts with other administrators. For more information on device locks, see "Device configuration locks" on page 69.

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.

Figure 169: Managing configuration changes



View Installation History	Select to display the installation record of the device, including the ID assigned by the FortiManager system to identify the version of the configuration file installed and the time and date of the installation. You can also view the installation history log and download the log file.
Retrieve	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.
Import	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 280.
Comments icon	Display the comment added to this configuration file when you edit the file name.
ID	A number assigned by the FortiManager system to identify the version of the configuration file saved on 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. See "To view the configuration settings on a FortiGate unit" on page 279 and "To download a configuration file to a local computer" on page 279.
Name	A name added by the user to make it easier to identify specific configuration versions. You can select a name to edit it and add comments.
Created by	The time and date when the configuration file was created, and the person who created the 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.
Diff icon	Show only the changes or differences between two versions of a configuration file. See "Comparing different configuration files" on page 280 for more details.
Delete icon	Delete this version from the repository. You cannot delete a version that is currently active on the FortiGate unit.
Revert icon	Revert the current configuration to the selected revision. FortiManager tags the reverted configuration with a new ID number. For example, if you are currently running version 9 and revert to version 8, a new revision, version 10, is created at the top of the list. See "To revert to another configuration file" on page 281.

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

To view the configuration settings on a FortiGate unit

1. In the left pane, go to *System* > *Status* > *Status* > *Revision History*.
2. Select the *ID* for the revision you want to see.

   You are automatically redirected to the View Configuration page.
3. Select *Return* when you finish viewing.

You can download the configuration settings if you want by selecting Download on the View Configuration page. For more information, see "Downloading and importing a configuration file" on page 279.

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

1. In the left pane, go to *System* > *Status* > *Status* > *Revision History*.
2. Select the *Name* for the version you want to change.
3. Enter a name in the *Tag (Name)* field.
4. Optionally, enter information in the *Comments* field.
5. Select *OK*.

Downloading and importing a configuration file

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

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

Note: 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. In the left pane, go to *System* > *Status* > *Status* > *Revision History*.
2. Select the *ID* for the revision you want to download.

3 Select the *Download* button.

You may need to drag the scroll bar to the very right to see the button.

4 Select *Regular* or *Encrypted* download type. If you select *Encrypted Download*, enter a password.

5 Select *OK*.

6 Specify a location to save the configuration file on the local computer.

7 Select *Save*.

To import a configuration file from a local computer

1 In the left pane, go to *System* > *Status* > *Status* > *Revision History*.

2 Select *Import*.

3 Select the location of the configuration file or choose *Browse* to locate the file.

4 If the file is encrypted, select the *File is Encrypted* check box and enter the password.

5 Select *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 Configuration tab 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 In the left pane, go to *System* > *Status* > *Status*.

2 On the Status page, locate the Configuration and Installation Status widget.

3 In the *Diff with Saved Revisions* row, select the *Revision Diff* icon.

4 Select either the previous version or specify a different configuration version to compare in *Diff From*.

5 Select whether to display the full configuration file (*Full Content*) or only the differences (*Diff Only*) in *Output*.

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

6 Select *Apply*.

The configuration differences are displayed in colored highlights:

To revert to another configuration file

1 In the left pane, go to *System* > *Status* > *Status* > *Revision History*.

2 Select the *Revert* icon for the revision you want to revert to.

3 Select *OK*.

A new revision is added to the top of the list.

Real-Time Monitor

The Real-Time Monitor (RTM) helps you watch your managed devices for trends, outages, or events that require attention. The RTM can be used to monitor any chassis, FortiGate, or FortiAnalyzer device or device group. Where you would normally log on to each individual device to view system resources and information, you can view that same information for all your devices in the RTM.

In the RTM, all actions and configurations are by device. The FortiManager system reads all of its information from the devices via SNMP traps and variables. SNMP traps and variables provide access to a wide array of hardware information from percent of disk usage to an IP address change warning to the number of network connections. SNMP must be properly configured on both the devices and your FortiManager system for this information to be accessible. For more information on SNMP traps, SNMP variables, and FortiManager system SNMP settings, see “SNMP” on page 51.

The two main parts of RTM are monitoring and alerts. You can use monitoring to view the status information for one or more managed devices. Alerts inform you when an important event occurs on a device, such as a hard disk getting too full. Generally alerts require your attention; in all cases alerts can generate email alerts, log messages or SNMP traps.

To see and change RTM settings, your administrator profile must have RTM enabled. This includes RTM Dashboard, Global, and general RTM settings. For information on administrator profiles, see “Administrator profile” on page 63.

The following topics are included in this section:

RTM monitoring

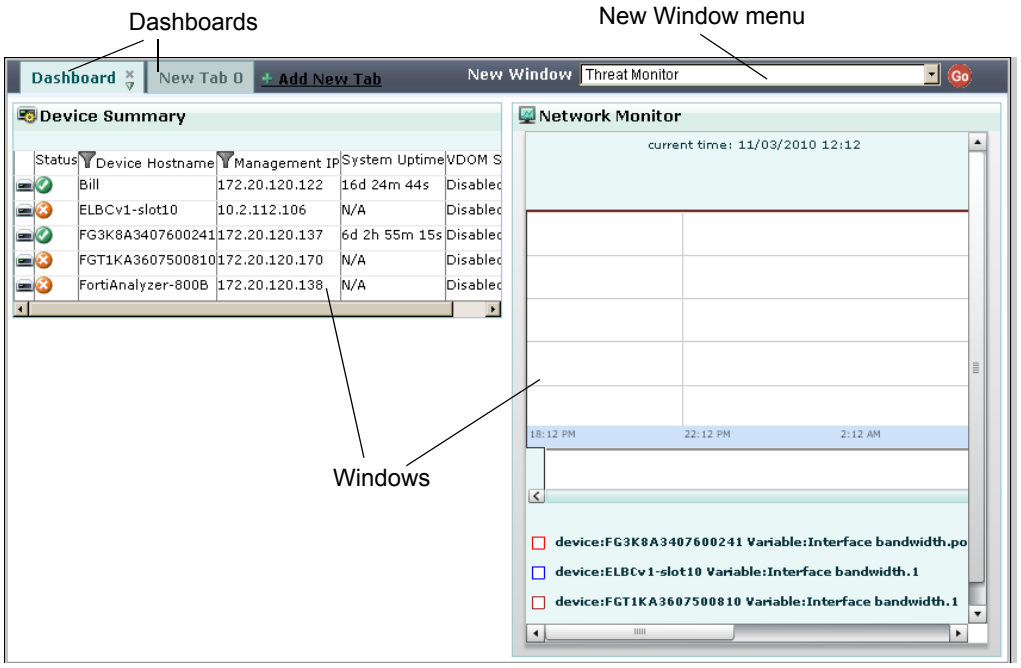
Using RTM monitoring, you can display the RTM dashboard to view the current status of managed devices and monitor alert messages such as Device Properties or Alerts, SNMP Traps, and Device Reachability generated by the devices.

RTM Dashboards

Selecting *Real-Time Monitor* > *Monitoring* > *Dashboards* > *Dashboards* takes you to the RTM dashboard. RTM dashboards display the current status of managed devices using pre-configured and customizable windows. You can customize RTM dashboards by adding or removing windows and by customizing each window. You can also create multiple dashboards for different kinds of status information and different devices.

Note: When navigating the RTM dashboard, your browser must allow pop-up windows. If not, you will not be able to view many of the configuration screens.

Figure 170: Example RTM Dashboards



RTM Windows	Informational displays including pre-defined and custom resource monitors and alerts shown on the main section of the RTM dashboard.
Dashboards	Select a dashboard to display the windows in that separate display area. Select *Add New Tab* to add a new dashboard. Select the X on a dashboard tab to delete it. Select the arrow on a dashboard tab to switch between one and two column display. For more information, see "Adding and configuring dashboards" on page 284.
New Window	Select an RTM window and select *Go* to configure and add the window to the current dashboard. You can add multiple instances of some windows to a dashboard. The window names are: • Device Summary • Status Console • Resource Monitor • Network Monitor • Threat Monitor • Trap Monitor • Import Shared Monitor/Status Console/Trap Monitor • Clear Dashboard For more information, see "About RTM windows" on page 285.

Adding and configuring dashboards

You can add up to seven Dashboards

To add a new dashboard

1. Go to *Real-Time Monitor* > *Monitoring* > *Dashboards* > *Dashboards* and select *Add New Tab*.
2. Enter a name for the dashboard. The name can be up to 10 characters long.
3. Repeat these steps to create additional dashboards.
4. You can add up to 10 dashboards.

To delete a dashboard

1 Select the dashboard to delete and then select the X on the tab.

If you hold down the Shift key while deleting a dashboard, the windows on that dashboard are moved the previous dashboard.

To add windows to a dashboard

1 Select a dashboard.
2 Select a window from the New Window list and select Go.
3 Configure the window and select OK to add it to the dashboard.
4 Drag the window to a different location in the dashboard if required

To move a window from one dashboard to another

1 Select the dashboard that contains the window to be moved.
2 Drag the window title bar to the destination dashboard tab.
3 When you see a red outline around the dashboard tab, drop the window into that dashboard by releasing the mouse button.
4 Arrange the windows in the dashboards are required.

To rename a dashboard

1 Double click on the name.
2 Enter the new name.
3 Click outside the name.

About RTM windows

Select the New Window menu to add pre-defined or custom display windows to a dashboard.

On selecting the New Window menu, a menu will be displayed with the available types of displays for you to choose from:

- Device Summary
- Status Console
- Resource Monitor allows you to monitor CPU, memory, and HDD usage.
- Network Monitor allows you to monitor interface bandwidth, session monitor, IPSec bandwidth, SSL VPN bandwidth, P2P bandwidth, emails per second, URLs per second, FTP transfers per second, and IM messages per second.
- Threat Monitor allows you to monitor emails versus spam, and URLs allowed versus blocked.
- Trap Monitor
- Import Shared Monitor/Status Console/Trap Monitor
- Clear Dashboard - remove all windows and dashboards

Each RTM window's top border includes controls to:

- minimize or maximize the window
- edit the window (not available on all displays)
- enlarge the window (on monitor only)
- set the refresh value

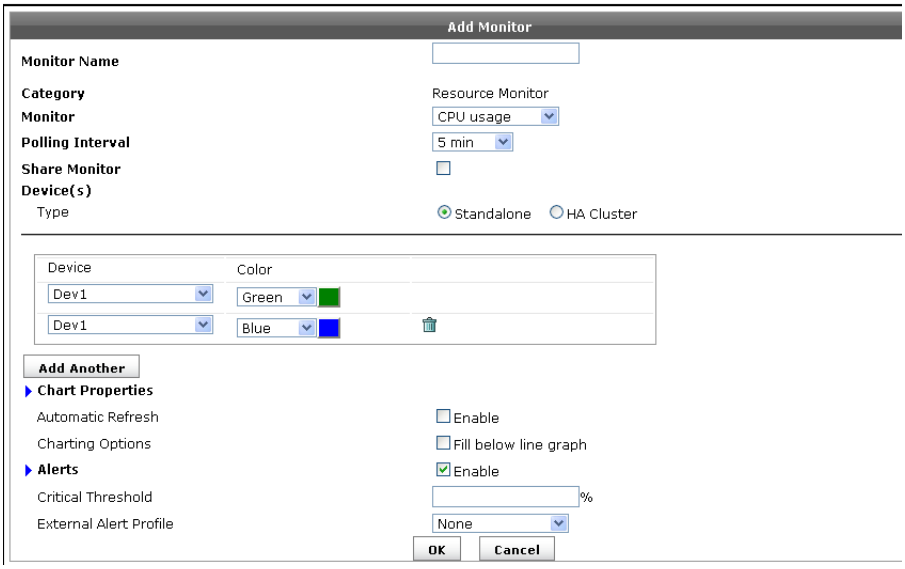
- refresh the window
- close the window

Resource, network, and threat monitors

A monitor allows you to watch the status of a variable associated with one or more monitored devices, such as CPU usage. You can set a high-water mark, or threshold, that will alert you when the device reaches a state that requires attention.

Go to *Real-time Monitor* > *Monitoring* > *Dashboard* > *New Window*. Select one of Resource, Network, or Threat Monitor and select *Go*.

Figure 171: Add Monitor window



Monitor Name	Enter the name that will be displayed in the title bar for this monitor. Do not use punctuation.
Category	This is a Resource Monitor. If you are adding a new Network Monitor or Threat Monitor that will be the category.
Monitor	Select the variable to monitor.
Polling Interval	Select how frequently to request information from the monitored device. Polling more often generates more data but slows down the device a bit. You can select one of the intervals listed in the drop-down list, or select *Specify* to enter your own interval in seconds.
Share Monitor	Select to make this monitor available to other administrators.
Device(s)	
Type	Select one of Standalone or HA Cluster.
Device	Select the monitored device from the drop-down list.
Color	Select the color that will represent this device on the monitor graph.
Delete Icon	Select to remove this device from this monitor.
Add Another	Select to add another device to this monitor.
Chart Properties	

Automatic Refresh	Select to enable automatic refresh for this monitor. It will automatically refresh the display when there is new information to display.
Charting Options	Select to fill the graph with the color for that device below the monitored line for that device.

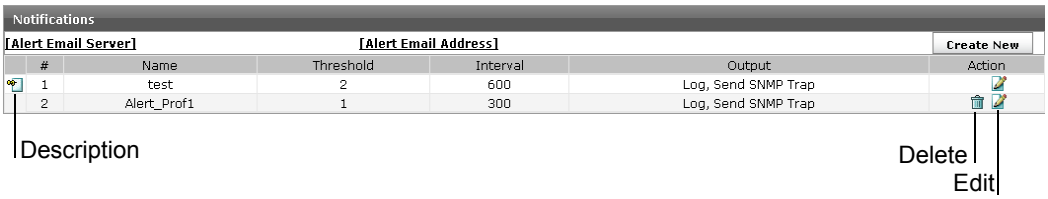
Alerts

Critical Threshold	Enter the percentage or value that indicates this variable has reached critical levels. For example, 90% CPU usage is a critical level.
External Alert Profile	Select an Alert Profile from the drop-down list. At least one Alert Profile must be configured before you can select it. Select *[Create New...]* to create a new Alert Profile. For more information, see "Adding alert profiles" on page 289.

RTM alert notifications

Go to *Real-Time Monitor* > *Monitoring* > *Dashboards* > *RTM Alerts Event* to configure administrator notifications. This includes configuring the alert email server, and alert email addresses. You can also create alert profiles.

Figure 172: RTM Notification



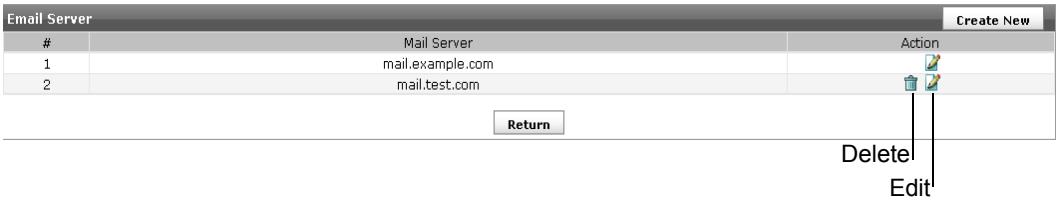
Alert Email Server	Configure the alert email server to send notifications. For more information, see "Alert email server" on page 287.
Alert Email Address	Define email addresses to send notifications to. For more information, see "Alert email address" on page 289
Create New	Select to create an alert profile. For more information, see "Adding alert profiles" on page 289.
Description Icon	Mouse over this icon for a description of this alert.
#	The order the alerts were created.
Name	The name of the alert profile.
Threshold	The number of events that must occur in the given interval before it is reported.
Interval	The period of time in seconds during which if the threshold number is exceeded, the event will be reported.
Output	Shows the notification medium for this alert as Log, Email, or Send SNMP Trap. Any or all three can be selected.
Delete icon	Select to remove an alert profile. This icon does not appear if the alert profile is used in a monitor.
Edit	Select to modify this alert profile.

Alert email server

Go to *Real-Time Monitor* > *Monitoring* > *Dashboards* > *RTM Alerts Event* > *Alert Email Server* to configure the FortiManager system to use an SMTP email server to send alert email to designated recipients when monitored data exceeds threshold settings.

Alert email must be configured before you can configure an alert to send you an alert message. You must also configure alert recipient email addresses in “Alert email address” on page 289.

Figure 173: Email server list



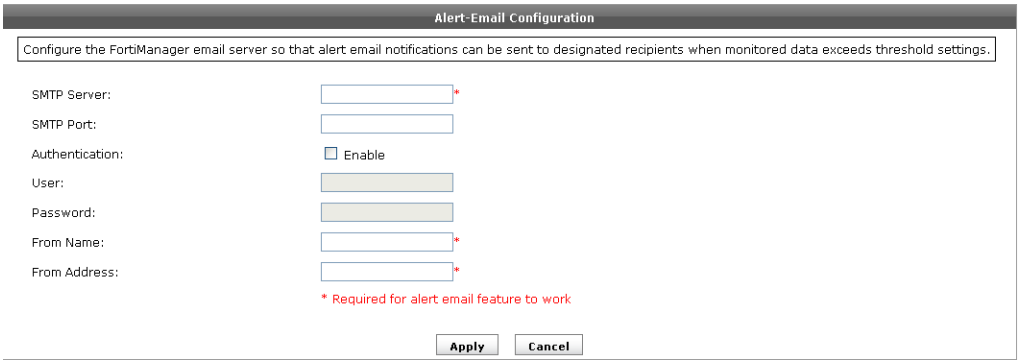
#	The order the servers were created.
Mail Server	The fully qualified domain name of the email server.
Delete icon	Select to remove a server. This icon does not appear if the email server is used in an alert profile.
Edit	Select to modify this alert profile.

To configure the alert email server

1 Go to *Real-Time Monitor* > *Monitoring* > *Dashboards* > *RTM Alerts Event* > *Alert Email Server*.

2 Select Create New.

Figure 174: Alert email configuration



SMTP Server	Enter the IP address or fully qualified domain name of the SMTP server. This field is required.
SMTP Port	Enter the TCP port for the SMTP server. The default is 25.
Authentication	Select to enable authentication on the SMTP server if it is required.
User	Enter the user account name for authentication to the SMTP server. This field is available only if Authentication is enabled.
Password	Enter the password for authentication to the SMTP server. This field is available only if Authentication is enabled.
From Name	Enter the name to present in the From field of the alert email. This field is required.
From Address	Enter the From email address the alert email is sent from. This field is required.

3 Select *Apply*.

Alert email address

Go to *Real-Time Monitor* > *Monitoring* > *Dashboards* > *RTM Alerts Event* > *Alert Email Address* to configure the email addresses that receive notification of alerts.

Alert email addresses should include those of the administrators and technicians who will be addressing any network issues. It may be useful to email to an account for logging purposes as well.

Select *Create New* to enter a new email address.

Select the Edit icon to change an existing email address.

Select the Delete icon to discard an existing email address. This icon does not appear if the email address is used in an alert profile.

Adding alert profiles

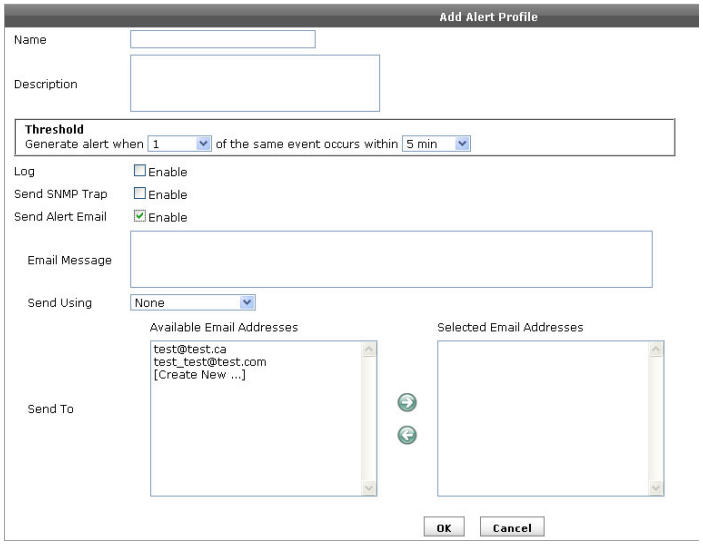
With an alert profile, you can define the threshold that triggers an alert notification and select the notification medium for the alert as log, email, or snmp trap.

To add an alert profile

1 Go to *Real-Time Monitor* > *Monitoring* > *Dashboards* > *RTM Alerts Event*.

2 Select *Create New*.

Figure 175: Adding alert profiles



Name	Enter a unique name for the alert profile.
Description	Optionally, enter some notes or comments for this alert profile.
Threshold	Enter the number of events that must occur in the given interval before an alert is generated.
Log	Select *Enable* if you want to send the alert to a Syslog server. You must configure the Syslog server to make this function work. For more information, see “Configuring alerts by Syslog server” on page 294.
Send SNMP Trap	Select *Enable* if you want to send SNMP traps when the alert occurs. You must configure the SNMP server to make this function work. For more information, see “Configuring SNMP traps and alerts” on page 293.

Send Alert Email	Select *Enable* if you want to send email messages when the alert occurs.	
	Email Message	Enter the content for the alert email.
	Send Using	Select the email server for sending the message. If there are no servers available, you can select [Create New...] to add a server. For more information, see "Alert email server" on page 287.
	Send To	In the *Available Email Addresses* field, select the email address(es) to which you want to send the alert email messages. Use the right-pointing arrow to move them into the *Selected Email Addresses field*. If there are no email addresses available, you can select [Create New...] to add one For more information, see "Alert email address" on page 289.

3 Select *OK*.

FortiManager system alerts

Alerts provide a way to inform you of important issues that may arise on your devices and the FortiManager system itself based on the log messages that the FortiManager system collects. These alerts may be system failures or network attacks. By configuring alerts, you can easily and quickly react to such issues.

Alerts event

Alert events define log message types, severities and sources which trigger administrator notification.

You can choose to notify administrators by email, SNMP, or Syslog.

To view configured alert events, go to *Real-Time Monitor* > *Alerts* > *Alerts Event*.

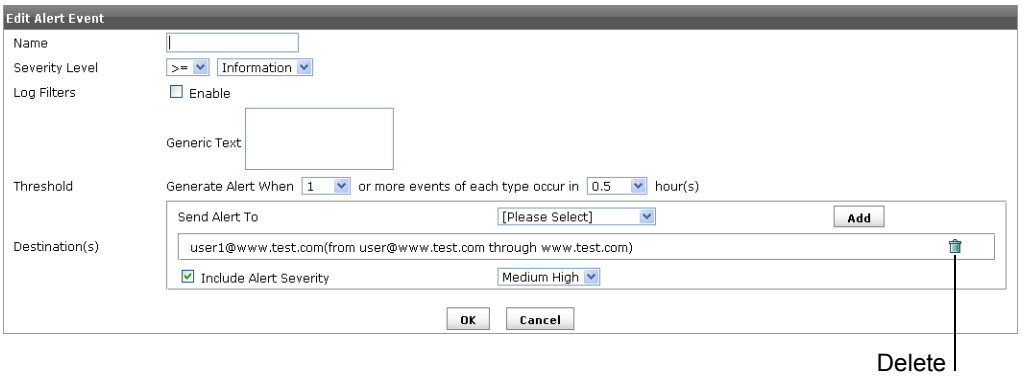
Figure 176: Viewing alert events

Create New	Select to add a new alert event. For more information, see "To add an alert event" on page 290.
#	The order the alert events were created.
Name	The name of the alert event.
Threshold	The number of events that must occur in the given interval before an alert is generated.
Destination	The location where the FortiManager system sends the alert message. This can be an email address, SNMP Trap or syslog server.
Delete icon	Select to remove an alert event.
Edit icon	Select to modify an alert event.

To add an alert event

1 Go to *Real-Time Monitor* > *Alerts* > *Alerts Event* and select *Create New*.

Figure 177: Adding alert events



Name	Enter a unique name for the alert event.
Severity Level	Select the severity level to monitor for within the log messages, such as >=, and the severity of the log message to match, such as *Critical.* For example, selecting *Severity Level* >= *Warning*, the FortiManager system will send alerts when an event log message has a level of *Warning, Error, Critical, Alert* and *Emergency*. These options are used in conjunction with *Log Filters* to specify which log messages will trigger the FortiManager system to send an alert message.
Log Filters	Select *Enable* to activate log filters, and then enter log message filter text in the *Generic Text* field. **This text is used in conjunction with** *Severity Level* **to specify which log messages will trigger the FortiManager system to send an alert message.** Enter an entire word, which is delimited by spaces, as it appears in the log messages that you want to match. Inexact or incomplete words or phrases may not match. For example, entering log_i or log_it may not match; entering log_id=0100000075 will match all log messages containing that whole word. Do not use special characters, such as quotes (‘) or asterisks (*). If the log message that you want to match contains special characters, consider entering a substring of the log message that does not contain special characters. For example, instead of entering `User 'admin' deleted report 'Report_1'`, you might enter `admin`.
Threshold	Set the threshold or log message level frequency that the FortiManager system monitors before sending an alert message. For example, set the FortiManager system to send an alert only after it receives five emergency messages in an hour.
Destination	Select the location where the FortiManager system sends the alert message.
Send Alert To	Select an email address, SNMP trap or Syslog server from the list. You must configure the email server and address, SNMP traps, or Syslog server before you can select them from the list. For information on email server configuration, see For information on configuring SNMP traps, see For information on configuring Syslog servers, see
Include Alert Severity	Select the alert severity value to include in the outgoing alert message information.
Add	Select to add the destination for the alert message. Add as many recipients as required.
Delete icon	Select to remove a destination.

2 Select *OK*.

Configuring alerts

When the FortiManager system receives a log message meeting the alert event conditions, it sends an alert message as an email, syslog message or SNMP trap, informing an administrator of the issue and where it is occurring.

You can configure the methods the FortiManager system uses to send alert messages. The FortiManager system can send an alert message to an email address via SMTP, a Syslog server or as an SNMP trap.

Configuring alerts by email server

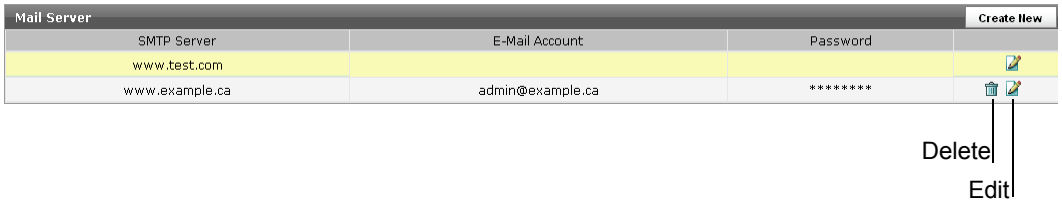
You must first configure an SMTP server to allow the FortiManager system to send email alert messages.

If the mail server is defined by a domain name, the FortiManager system will query the DNS server to resolve the IP address of that domain name. In this case, you must also define a DNS server. See “Configuring DNS” on page 61 to configure a DNS server.

If sending an email by SMTP fails, the FortiManager system will re-attempt to send the message every ten seconds, and never stop until it succeeds in sending the message, or the administrator reboots the FortiManager system.

To view configured mail servers, go to *Real-Time Monitor* > *Alerts* > *Alerts Config* > *Mail Server*.

Figure 178: Mail server list

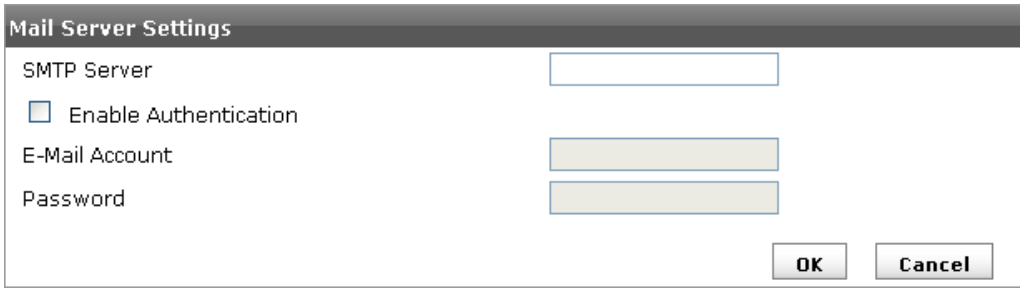


Create New	Select to add a new mail server. For more information, see “To add a mail server” on page 292.
SMTP Server	The SMTP server you have added.
E-Mail Account	The email address used for accessing the account on the SMTP server.
Password	The password used in authentication of that server. The password displays as ******.
Delete icon	Select to remove a mail server. This icon does not appear if the mail server is used by an alert event.
Edit icon	Select to modify a mail server.

To add a mail server

1 Go to *Real-Time Monitor* > *Alerts* > *Alerts Config* > *Mail Server* and select *Create New*.

Figure 179: Adding mail servers



SMTP Server	Enter the name/address of the SMTP email server.
Enable Authentication	Select to enable SMTP authentication. When set, you must enter an email address and password for the FortiManager system to send an email with the account.
Email Account	Enter the user name for logging on to the SMTP server to send alert mails. You only need to do this if you have enabled the SMTPauthentication. The account name must be in the form of an email address, such as user@example.com.
Password	Enter the password for logging on to the SMTP server to send alert email. You only need to do this if you enabled SMTP authentication.

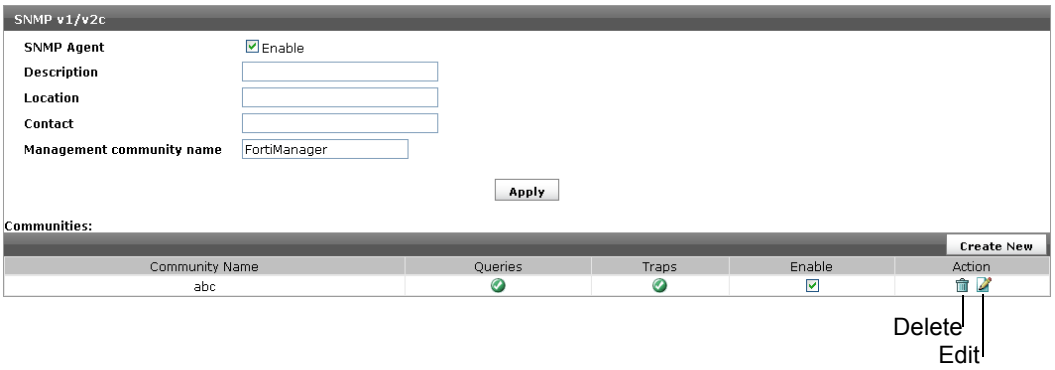
2 Select *OK*.

Configuring SNMP traps and alerts

You can configure the SNMP server where the FortiManager system sends SNMP traps when an alert event occurs, and which SNMP servers are permitted to access the FortiManager SNMP system traps. You must add at least one SNMP server before you can select it as an alert destination.

To view configured SNMP servers, go to *Real-Time Monitor* > *Alerts* > *Alerts Config* > *SNMP Access List.*

Figure 180: SNMP access list



SNMP Agent	Select to enable the FortiManager SNMP agent. When this is enabled, it sends FortiManager SNMP traps.

Description	Enter a description of this FortiManager system to help uniquely identify this unit.
Location	Enter the location of this FortiManager system to help find it in the event it requires attention.
Contact	Enter the contact information for the person in charge of this FortiManager system.
Management Community Name	Enter the name to use for the community created by the FortiManager system during configuration of new FortiGate devices. The default value is FortiManager. This field can be a maximum of 127 characters long.
Communities	The list of SNMP communities added to the FortiManager configuration.
Create New	Select to add a new SNMP community. If SNMP Agent is not selected, this control will not be visible. For more information, see "Configuring an SNMP Community" on page 53.
Community Name	The name of the SNMP community.
Queries	The status of SNMP queries for each SNMP community.
Traps	The status of SNMP traps for each SNMP community.
Enable	Select to enable or unselect to disable the SNMP community.
Delete icon	Select to remove an SNMP community.
Edit icon	Select to edit an SNMP community.

Configuring alerts by Syslog server

You can configure Syslog servers where the FortiManager system can send alerts. You must add the syslog server before you can select it as a way for the FortiManager system to communicate an alert.

To view the Syslog servers, go to *Real-Time Monitor* > *Alerts* > *Alerts Config* > *Syslog Server*.

Figure 181: Syslog server list

Create New	Select to add a new Syslog server. For more information, see "To add a mail server" on page 292.
#	The order the Syslog server was created.
Name	The IP address or fully qualified domain name for the Syslog server, and port number.
Delete icon	Select to remove a Syslog server. This icon does not appear if the Syslog server is used by an alert event.
Edit icon	Select to modify a Syslog server.

To add a Syslog server

1. Go to *Real-Time Monitor* > *Alerts* > *Alerts Config* > *Syslog Server*.
2. Select *Create New*.
3. Enter the server name, IP address or FQDN, and port number.

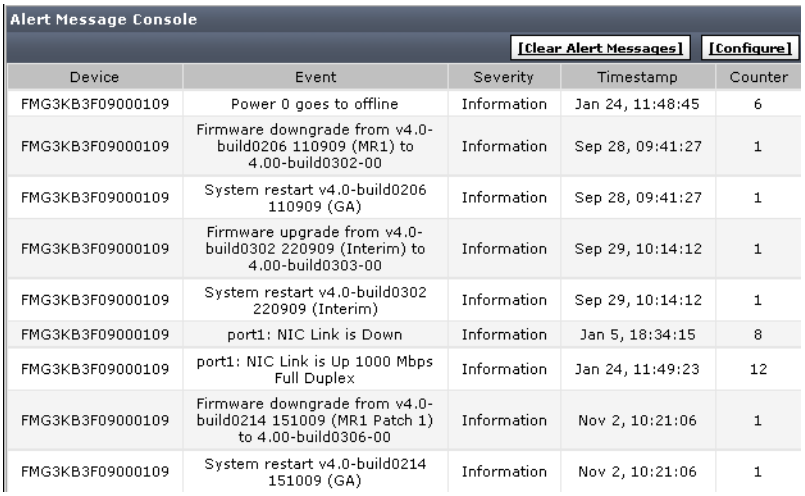
4 Select *OK*.

Alert console

The alert message console displays alert messages for the FortiManager system and connected devices, including hard disk failure messages, virus outbreak, or suspicious event warnings.

To view the alert console messages, go to *Real-Time Monitor* > *Alerts* > *Alert Console.*

Figure 182: Alert message console


Alert Message Console

[Clear Alert Messages] [Configure]

Device	Event	Severity	Timestamp	Counter
FMG3KB3F09000109	Power 0 goes to offline	Information	Jan 24, 11:48:45	6
FMG3KB3F09000109	Firmware downgrade from v4.0-build0206 110909 (MR1) to 4.00-build0302-00	Information	Sep 28, 09:41:27	1
FMG3KB3F09000109	System restart v4.0-build0206 110909 (GA)	Information	Sep 28, 09:41:27	1
FMG3KB3F09000109	Firmware upgrade from v4.0-build0302 220909 (Interim) to 4.00-build0303-00	Information	Sep 29, 10:14:12	1
FMG3KB3F09000109	System restart v4.0-build0302 220909 (Interim)	Information	Sep 29, 10:14:12	1
FMG3KB3F09000109	port1: NIC Link is Down	Information	Jan 5, 18:34:15	8
FMG3KB3F09000109	port1: NIC Link is Up 1000 Mbps Full Duplex	Information	Jan 24, 11:49:23	12
FMG3KB3F09000109	Firmware downgrade from v4.0-build0214 151009 (MR1 Patch 1) to 4.00-build0306-00	Information	Nov 2, 10:21:06	1
FMG3KB3F09000109	System restart v4.0-build0214 151009 (GA)	Information	Nov 2, 10:21:06	1

Clear Alert Messages	Select to remove all alert messages.
Configure	Select to configure alert console settings including the period during which you want to display the messages and the severity level of the messages to be displayed. For example, selecting severity level *Warning* will display messages that have a level of *Warning, Notification,* and *Information*.
Time	The date and time of the alert message.
Device	The device where the alert message originates.
Severity	The severity level of the alert message.
Event	The event causing the alert message.
Message	Details of the alert message.

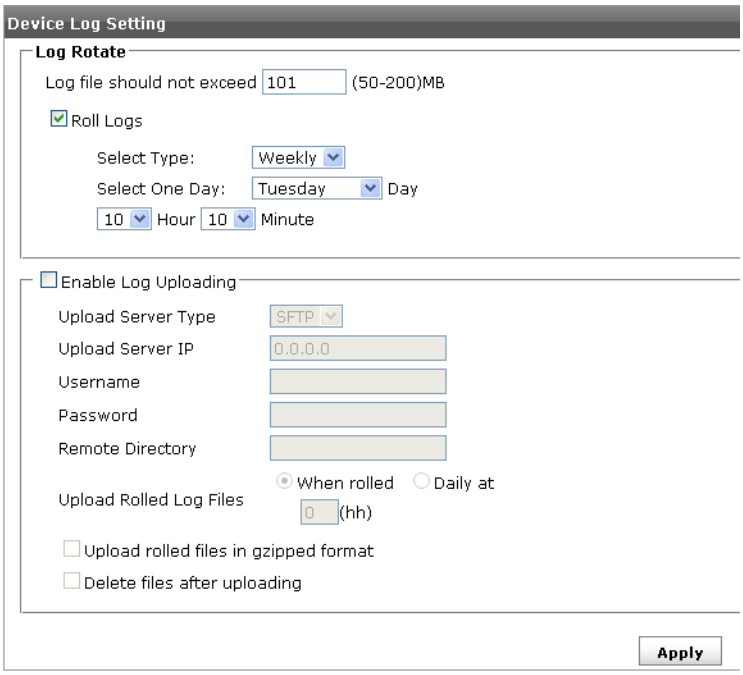
Device Log

Information collected as part of Real-Time Monitor is saved to the Device Log. The Device Log is different from the FortiManager system logs. For more information on FortiManager system logs, see “Local log settings” on page 71.

Device log setting

Go to *Real-Time Monitor* > *Device Log* > *Log Setting*.

Figure 183: Device Log Setting



Log file should not exceed	Enter the maximum log size in MegaBytes.
Roll Logs	Select to roll the logs. Rolling will occur either on a weekly or daily basis as selected.
Type	Select to roll the logs on a weekly or daily basis.
One Day	Select the day of the week to roll the logs. This option is enabled only when *Roll Logs* is selected and the *Type* is Weekly.
Hour, Minute	Select the Hour and Minute of the day to roll the logs. The hour is based on a 24 hour clock.
Enable Log Uploading	Select to upload realtime device logs.
Upload Server Type	Select one of FTP, SFTP, SCP, or FAZ.
Upload Server IP	Select the IP address of the upload server.
Username	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.
When Rolled	Select to upload log files when they are rolled according to settings selected under *Roll Logs*.
Daily at	Select the hour to upload the logs. The hour is based on a 24 hour clock.
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.

Device log access

Go to *Real-Time Monitor* > *Device Log* > *Log Access*.

Accessing the device log follows the same method as accessing the FortiManager system logs. For more information see, “Log access” on page 75.

FortiAnalyzer Devices

You can remotely manage and use a FortiAnalyzer unit while logged in to the FortiManager system. You can also configure your FortiGate units that are remotely managed by the FortiManager system to log to the remotely managed FortiAnalyzer unit.

This section includes the following topics:

Connecting to the FortiAnalyzer unit

Before connecting a FortiAnalyzer unit, contact the FortiAnalyzer administrator. You should also verify the following before connecting to a FortiAnalyzer unit:

- Web services are enabled for that FortiAnalyzer network interface.
- The FortiAnalyzer unit is configured to accept connections and data from the FortiManager unit.
- The FortiAnalyzer unit's device list does not currently contain another FortiManager unit.

If you require a secure tunnel between the two devices, the FortiAnalyzer administrator must also add (register) the FortiManager unit to the FortiAnalyzer device list, and configure the secure tunnel; the secure connection cannot be configured automatically, even if the Unregistered Device Options on the FortiAnalyzer unit are configured to permit connections from unregistered devices.

Before you can remotely manage and use a FortiAnalyzer unit, you need to register and connect the FortiAnalyzer unit with the FortiManager system and each device must be included in their respective device lists. For example, a FortiAnalyzer administrator will add the FortiManager unit to the FortiAnalyzer device list, and a FortiManager administrator would add the FortiAnalyzer unit to the FortiManager device list.

Before proceeding, if you have previously configured FortiAnalyzer connection settings, verify that the connection is enabled. For more information see "System Settings" on page 41. If the connection is enabled, proceed to "Using the FortiAnalyzer unit from within Device Manager" on page 301.

Caution: Back up the FortiAnalyzer configuration before adding a FortiManager unit to the FortiAnalyzer device list. When you add a FortiManager unit, all FortiGate devices and groups configured with the FortiManager unit will also be automatically added to the FortiAnalyzer unit's device list, overwriting any duplicate entries.

Changing a device's FortiAnalyzer settings clears sessions to its FortiAnalyzer unit's IP address. If the FortiAnalyzer unit is behind a NAT device, such as a FortiGate unit, this also resets sessions to other hosts behind that same NAT device. To prevent disruption of other devices' traffic, on the NAT device, create a separate virtual IP for the FortiAnalyzer unit.

To add a FortiAnalyzer unit

1 From the Main Menu Bar, select *Add Device*.

2 In the *Add New Device* window, complete the following fields:

IP Address	Enter the IP Address of the device you want to add. The FortiManager system uses the IP address to find and retrieve the configuration data from the device.
Name	Enter a unique name for the device.
Device type	Select the type of device you want to add: FortiGate, FortiSwitch, FortiGate Carrier, FortiMail, or FortiAnalyzer.
Admin User	Select one of the following:
Default (admin)	Select if the device uses the default "admin" as its admin user. For more information, see "Configuring administration settings" on page 61.
Other	Select and then enter the admin user name if the device uses a different user name.
Password	Enter the administration password. This is the password used to log in to the administrator account on the device.
ADOM	Select the ADOM to which the device binds. For more information, see "Administrative Domains" on page 33.
Select Groups	Select the group(s) that you want this device to belong to from the *Group List* field and use the right-pointing arrow to move it to the *Selected Group(s)* field. All groups that you have created for the device type will display in the *Group List* field.
City	Enter the name of the city where the FortiAnalyzer is located.
Company/Organization	Enter the name of the company or organization that owns the FortiAnalyzer.
Contact	Enter a contact's name and the phone number.
Country	Enter the name of the country.
Province/State	Enter the name of the province or the state.
Device Information	Select one of the following:
Auto Discover	Select, then select *Discover* for the FortiManager system to search for the device.
Specify	Select to manually enter the searching parameters: **Firmware Version** **MR Build No.** - the Maintenance Release build number **Device Model** **SN** - Serial Number of the device **Hard Disk Installed** - presence of a hard disk on the device.
Discover	In combination with *Auto Discover*, select to search for the device. The discovered device information appears.
Description	Add any notes or comments you have for this device.

3 Select *OK* to add the device.

To connect to the FortiAnalyzer unit

1 Go to *Device Manager*.

2 Select *FortiAnalyzer*.

3 Select *FortiAnalyzer unit* in the right pane.

The FortiAnalyzer System screen opens and show the status details of the FortiAnalyzer. For information on the FortiAnalyzer, see the *FortiAnalyzer Administration Guide*.

For more information on enabling and configuring a secure connection, see `config log device` in the *FortiAnalyzer CLI Reference*.

The connection attempt will fail if:

- the device list on the FortiAnalyzer unit does not yet contain the FortiManager, and
- the Unregistered Device Options on the FortiAnalyzer unit are not configured to automatically accept the connection attempt, or are configured to ignore data.

In this case, manually add the FortiManager unit to the device list on the FortiAnalyzer unit, and then re-attempt the connection. For more information about adding a FortiManager unit to the device list on the FortiAnalyzer unit, see the *FortiAnalyzer Administration Guide*.

When the connection succeeds, a device named FortiAnalyzer appears in *Device Manager*, and FortiGate units managed by the FortiManager unit are automatically added to the device list on the FortiAnalyzer unit. By selecting the FortiAnalyzer device in the *Device Manager*, you can configure and use that FortiAnalyzer unit from within the FortiManager unit's web-based manager or CLI. For more information, see "Using the FortiAnalyzer unit from within Device Manager" on page 301 and "Synchronizing the FortiAnalyzer configuration" on page 302.

Adding devices to the FortiAnalyzer unit

After connecting to the FortiAnalyzer unit, you can use the FortiManager unit to remotely view logs and reports stored on the FortiAnalyzer unit. If you want to also allow devices in *Device Manager* to remotely log, quarantine, and/or retrieve reports from the FortiAnalyzer, register them with the device list on the FortiAnalyzer unit.

You can register a device in any of the following ways:

- Connect the FortiManager unit to the FortiAnalyzer unit (all devices in *Device Manager* are automatically registered with the FortiAnalyzer unit).
- In *Device Manager*, add the device to the FortiAnalyzer device list, then synchronize the new configuration to the FortiAnalyzer unit.
- Add the device to the FortiAnalyzer unit.

Note: Adding a device to the device list on the FortiAnalyzer unit configures the FortiAnalyzer unit to allow the connection – it does not configure the device to use the FortiAnalyzer. Depending on the method you use to add the device, you may also need to configure the device to use the FortiAnalyzer unit. For more information, see "Configuring devices" on page 217.

Using the FortiAnalyzer unit from within Device Manager

After registering the FortiAnalyzer and FortiManager units on each other's device lists, and the connection is established, you can perform FortiAnalyzer tasks while logged in to the FortiManager unit.

You can access the FortiAnalyzer unit in *Device Manager* by selecting the *FortiAnalyzer menu* and then selecting the FortiAnalyzer unit itself in the list on the page. For more information about FortiAnalyzer settings and configuration, see the *FortiAnalyzer Administration Guide*.

If you successfully connected the FortiManager to the FortiAnalyzer, but cannot access the FortiAnalyzer item within Device Manager, verify connectivity between the FortiAnalyzer unit and your computer. Remote administration through a FortiManager unit requires connectivity from your computer to both the FortiManager and FortiAnalyzer unit.

Synchronizing the FortiAnalyzer configuration

Similar to FortiGate devices, FortiAnalyzer configurations must be synchronized with the FortiManager unit because the FortiAnalyzer configuration can be modified either locally or remotely. Changes made to the FortiAnalyzer configuration, either locally or remotely, cause the other location to be out-of-date. For example, if you made changes remotely to the FortiAnalyzer configuration, locally the changes would not be noticed by the FortiManager unit.

- Local (on the FortiAnalyzer unit) configuration causes the FortiManager's copy of the FortiAnalyzer configuration to become out-of-date.
- Remote (through FortiManager's *Device Manager*) configuration causes the configuration on the FortiAnalyzer unit to become out-of-date.

Synchronization, either by reloading or installing FortiAnalyzer configurations, updates each location with your most current changes to the FortiAnalyzer configuration.

Applying configuration changes

When you apply the FortiAnalyzer configuration in *Device Manager*, you are applying it to the FortiAnalyzer unit itself.

To apply configuration changes

1. Go to *Device Manager* > *FortiAnalyzer*.
2. Select the FortiAnalyzer unit.
3. In that row, select *Install*.

   The following message appears:

   ```
   Are you sure you want to install configuration for the selected
   device(s)?
   ```

4. Select *OK*.

You can apply configuration changes to multiple FortiAnalyzer units at once by using the above procedure. Instead of selecting one FortiAnalyzer unit, select

FortiClient Manager

Use the FortiClient Manager to centrally manage FortiClient software running on computers (FortiClient computers). You must operate in EMS mode.

This section contains the following topics:

FortiClient Manager maximum managed computers

The maximum number of FortiClient computers that FortiClient Manager can support depends on which FortiManager model you have.

Table 13: FortiClient Manager maximum managed FortiClient computers by model.

FortiManager model	Maximum number of managed FortiClient computers
FMG-100/100C	2,500
FMG-400A	10,000
FMG-400B	10,000
FMG-3000B	100,000
FMG-3000C	120,000
FMG-5001A	100,000

The FortiManager system logs alerts when the number of managed FortiClient computers reaches 90 percent and 95 percent of the maximum. When the maximum is reached, the system raises an alert for every attempt to add another FortiClient computer. The FortiManager unit can continue to search for FortiClient computers, but it can add them only to the Temporary Clients list.

If the number of FortiClient computers that you want to support exceeds the capacity of your FortiManager unit, you can create a FortiClient Manager cluster of two or more FortiManager units. See “About FortiClient Manager clustering” on page 304.

About FortiClient Manager clustering

You can combine two or more FortiManager units into a FortiClient Manager cluster to manage a large number of FortiClient computers. One FortiManager unit is designated as the primary unit and all other units are secondary. The primary unit co-ordinates sharing of information amongst all units in the cluster. FortiClient Manager clustering uses TCP port 6028.

A managed FortiClient computer can log into any one of the units and receive its configuration information from that unit. Similarly, the administrator can log into any one of the units and modify the configuration of a FortiClient computer, even if that computer is connected to a different FortiManager unit.

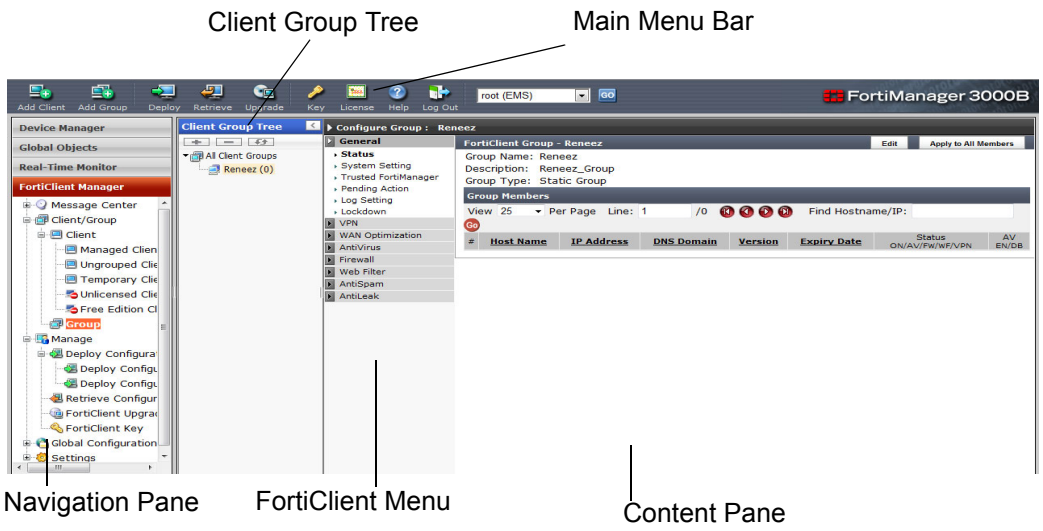
You must first select one FortiManager unit to act as the primary unit. After enabling clustering, register each secondary unit by entering its serial number and IP address. At each secondary unit, enable clustering and enter the IP address of the primary unit. For detailed information about configuring clustering, see “Configuring FortiClient Manager clustering” on page 331.

FortiClient Manager window

The FortiClient Manager window is similar to other components of the FortiManager web-based user interface — a Navigation Pane is presented on the left side of the FortiClient Manager window, and when you select objects in the Navigation Pane, information and/or configuration options are displayed in the Content Pane of the FortiClient Manager window.

To view and configure FortiClient settings, select FortiClient Manager in the Navigation Pane.

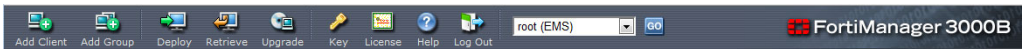
Figure 184: FortiClient Manager window - configuring a FortiClient computer.



Main Menu Bar

The Main Menu Bar for FortiClient Manager is different from the default Main Menu Bar. The buttons for Device Manager tasks are removed, and FortiClient Manager specific buttons are added.

Figure 185: FortiClient Main Menu Bar



Add Client	Select to add a FortiClient computer. See "Searching for FortiClient computers" on page 315.
Add Group	Select to add a group of FortiClient computers. See "Adding a FortiClient computer group" on page 320.
Deploy	Select to install the configuration changes to the FortiClient groups and clients. See "Deploying FortiClient computer configurations" on page 324.
Retrieve	Select to retrieve configurations from FortiClient computers and save them in the FortiManager unit. See "Retrieving a FortiClient computer configuration" on page 324.
Upgrade	Select to Manage retrieval and deployment of FortiClient software upgrades. See "Working with FortiClient software upgrades" on page 325.
Key	Select to assign license keys to FortiClient groups. See "FortiClient license keys" on page 326.
License	Select to enable Enterprise licensing instead of standard fixed licensing. See "Configuring enterprise license management" on page 340.
Help **Log Out** **ADOM drop down menu** **GO**	These buttons are the same as in the default Main Menu Bar. See "Main menu Bar" on page 82.

Navigation Pane

The FortiClient Manager portion of the Navigation Pane enables you to select and view the configuration options associated with FortiClient computers and groups.

Message Center

Dashboard	View status information about FortiClient Manager. See "Dashboard" on page 307.
Management Event	Select the tabs to view information. **Management Event Summary** — View a brief listing of recent alerts and messages. **Pending Action** — View pending actions for FortiClient computers. See "Viewing pending actions for FortiClient computers" on page 308. **Management Alert** — View a list of FortiClient computers that have licensing problems. See "Viewing management alerts for FortiClient computers" on page 309. **Management Event** — View Management events, such as settings changes. See "Management Event" on page 308.
Client Alert	Select the tabs to view information. **Client Alert Summary** — View a brief listing of recent alerts and messages. **Firewall Alert** - View firewall alerts for FortiClient computers. See "Viewing firewall alerts for FortiClient computers" on page 310. **Antivirus Alert** - View antivirus alerts for FortiClient computers. See "Viewing antivirus alerts for FortiClient computers" on page 311. **Upgrade Alert** - View information about failed FortiClient software upgrade attempts. See "Viewing upgrade alerts for FortiClient computers" on page 311.

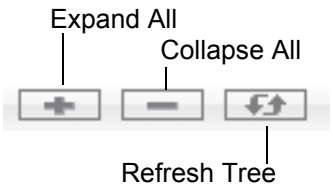
Client/Group	Add FortiClient computers and organize them into client groups. See "Working with Clients (FortiClient computers)" on page 312 and "Working with FortiClient groups" on page 318.
Client	Select this node to display all FortiClient computers managed by this FortiManager unit. This node is not visible to a FortiClient group administrator. There are four tabs: **Managed Client** - all managed clients. See "Viewing the clients lists" on page 312. **Ungrouped Client** - managed clients that do not belong to a client group. This node is not visible to a FortiClient group administrator that does not have access to ungrouped clients. **Temporary Client** - detected FortiClient computers that are not yet managed. This node is always empty if you selected the Client Discovery option Auto-populate managed clients list, which adds new clients to the Ungrouped Client node. This node is not visible to a FortiClient group administrator. **Unlicensed Client** - FortiClient computers with an expired or missing Enterprise license. **Free Edition Client** - FortiClient computers running the Free Edition and are without a license.
Group	Select this node to display the FortiClient Group list. You can use the Client Group Tree to quickly navigate to the group or client that you want to configure.
Manage	
Deploy Configuration	Install the configuration changes to the FortiClient groups and clients. See "Deploying FortiClient computer configurations" on page 324.
Retrieve Configuration	Retrieve configurations from FortiClient computers and save them in the FortiManager unit. See "Retrieving a FortiClient computer configuration" on page 324.
FortiClient Upgrade	Manage retrieval and deployment of FortiClient software upgrades. See "Working with FortiClient software upgrades" on page 325.
FortiClient Key	Assign license keys to FortiClient groups. See "FortiClient license keys" on page 326.
Global Configuration	
Web Filter Profile	Create web filter profiles that you can apply to users and groups. See "Viewing and editing web filter profiles" on page 328.
Settings	
System	**System Setting** — Configure FortiClient discovery and lockdown settings. See "Configuring FortiClient Manager system settings" on page 330. **Cluster Setting** — Configure settings to create a FortiClient Manager cluster. See "Configuring FortiClient Manager clustering" on page 331. **Email Alert Setting** — Configure sending of email messages for management alerts and management events. See "Configuring email alerts" on page 332.
LDAP Group/User	**LDAP Settings** — Configure settings to access LDAP servers. See "Configuring LDAP for web filtering" on page 334. **LDAP Group/User** - Assign web filter profiles to Windows AD users and groups. See "Working with Windows AD users and groups" on page 335.
Group Administration	Assign client groups to FortiClient group administrators. Available only to administrators with the Super_Admin profile. See "Configuring FortiClient group-based administration" on page 339.
Enterprise License	Enable Enterprise licensing instead of standard fixed licensing. "Configuring enterprise license management" on page 340.

Client Group Tree

When you go to *Client/Group* > *Group* in the FortiClient Manager, you see the Client Group Tree immediately to the right of the Navigation Pane. Client groups and their subgroups are clearly displayed. You can select a client group to configure. To provide more space in the Content Pane, you can collapse the Client Group Tree panel.

At the top of the client group tree is a toolbar that controls the appearance of the tree view.

Figure 186: Client Group Tree toolbar.



Expand All	Expand all nodes in the tree
Collapse All	Collapse All nodes in the tree
Refresh Tree	Update the tree from the FortiClient Manager database

FortiClient menu

When you select a client group or a FortiClient computer to configure, the FortiClient menu is visible at the left side of the Content Pane. You use the FortiClient menu to select different parts of the FortiClient configuration for editing.

The FortiClient menu and configuration pages differ from the FortiClient application. See "Configuring FortiClient computer settings" on page 343 for detailed information about configuring these settings.

Message Center

The Message Center provides status information about the FortiClient computers in your network.

- Dashboard — statistical information and recent activity
- Management Event — management events and alerts, pending actions
- Client Alert — client firewall, antivirus and update alerts

Dashboard

The FortiClient Manager dashboard provides the following information:

FortiClient Information	Provides counts of • managed clients (select count to see Managed Clients list) • managed clients currently online (number and percentage) • clients at risk due to disabled or outdated antivirus protection (number and percentage) • clients with firewall disabled
System Information	
Maximum Client Allowed	The maximum number of managed FortiClient computers. This depends on the FortiManager model. See "FortiClient Manager maximum managed computers" on page 303.

FortiManager provides AV update service	The status (enabled or disabled) of *FortiClient Service* in *FortiGuard AV & IPS Settings*. For more information, see "FortiGuard Center" on page 250.
FortiClient AV Version	The current antivirus engine and signatures versions provided by FortiGuard Center.
FortiClient Upgrade Package Available/Local	The number of FortiClient software upgrade packages available from FortiGuard and on this FortiManager unit. Select the count to view the FortiClient Upgrade page. See "Working with FortiClient software upgrades" on page 325.
Management Pending Actions	The number of pending actions on all managed FortiClient computers. Select the count to view the *All Pending Actions* list. For more information, see "Viewing pending actions for FortiClient computers" on page 308.
Recent Management Alert	The most recent management alerts. Click the >> button to view the *All Management Alert* list. For more information, see "Viewing management alerts for FortiClient computers" on page 309.
Recent Antivirus/Firewall Alert	A graph showing the number of antivirus and firewall alerts over the past week.
Recent Event Message	Recent event messages. Click the >> button to view the *All Event Logging* list. For more information, see "Management Event" on page 308.
Automatic refresh interval	Sets how often FortiClient Manager updates dashboard information.

Management Event

In FortiClient Manager, go to *Message Center* > *Management Event* to view:

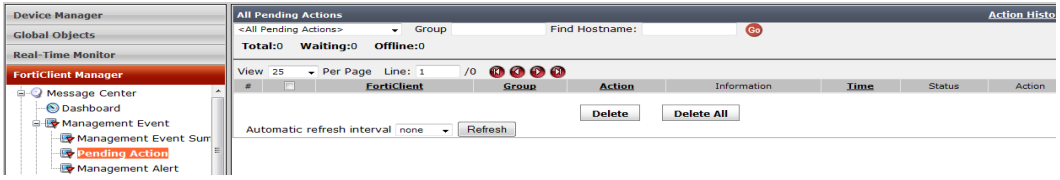
- pending actions
- management alerts
- management events

The Management Event Summary page shows lists of the most recent alerts and events. You can also view a count of the total pending actions. For more detailed information, click the >> button in the list title bar. You can also select the Pending Action, Management Alert and Management Event tabs at the top of the Content Pane.

Viewing pending actions for FortiClient computers

Go to *Message Center* > *Management Event* > *Pending Action* to view the All Pending Actions page. This page displays actions that cannot be executed instantly because the FortiClient computer is offline or otherwise unreachable. Actions are removed from the list as they are successfully completed.

Figure 187: Pending actions for FortiClient computers.



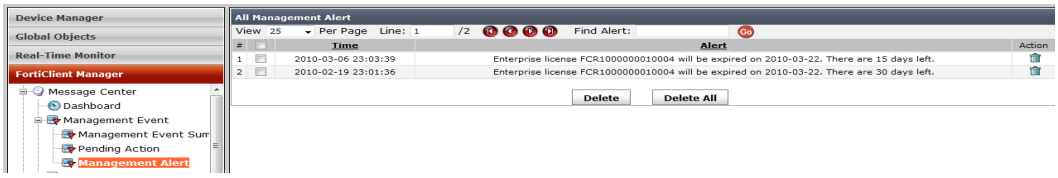
View per Page	Select the number of clients to display per page.
Line	Enter the line of the list that you want to view and select Go.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.

Next Page icon	Go to next page.
Last page icon	Go to last page.
Find Hostname	Enter the hostname and select *Go* to move to the first entry for the host.
#	Line numbers
FortiClient	The name of the FortiClient computer with pending action.
Action	The action items to be executed.
Information	The most up-to-date AV Signature/AV engine version numbers on the FortiManager unit. This information only applies to the Notify AV engine/database upgrading action.
Time	Date and time when the pending action item was created.
Delete	Delete the selected pending action manually.
Delete All	Delete all pending actions.

Viewing management alerts for FortiClient computers

In the FortiClient Manager, go to *Message Center* > *Management Event* > *Management Alert* to view a list of FortiClient computers that have licensing problems.

Figure 188: Management alerts list.



View per page	Select the number of lines to display per page: 25, 50, 100, or 1000
Line	Optionally, enter a line number and select Go to start the page with that line.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.
Find Alert	Optionally, enter search text and select Go.
#	Alerts are numbered in the order they occur.
Time	The time of the alert.
Alert	Description of the alert.
Action	Delete icon - Delete this alert.
Delete	Delete the selected alerts.
Delete All	Delete all the listed alerts.

Client Alert

Go to *Message Center* > *Client Alert* in FortiClient Manager to view the following messages from FortiClient computers:

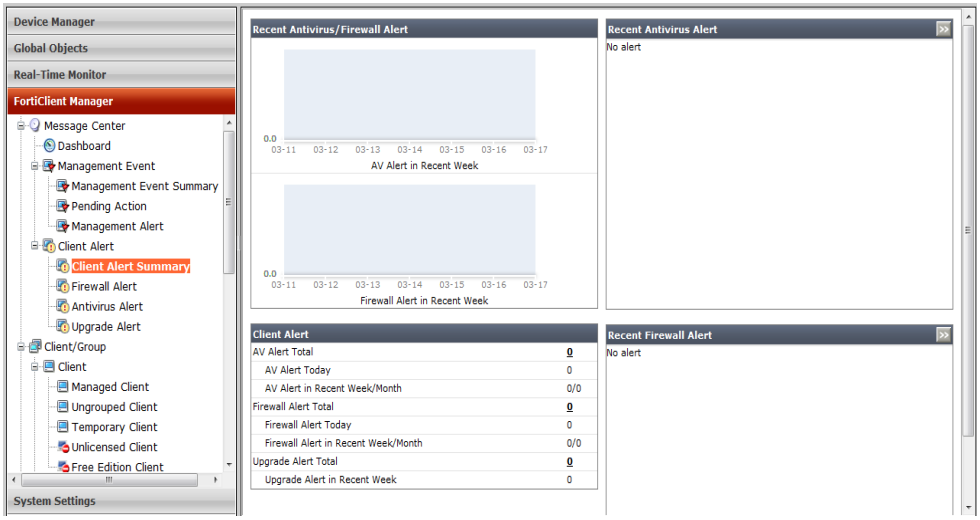
- firewall alerts
- antivirus alerts
- upgrade alerts

Client Alert Summary

The Client Alert Summary page shows lists of recent firewall and antivirus alerts. For more detailed information, select the >> button in the list title bar. You can also select the *Firewall Alert*, *Antivirus Alert* and *Upgrade Alert* tabs at the top of the Content Pane.

The Client Alert Summary page also shows statistical information about the number of alerts received from FortiClient computers. For more detailed information, select the count. For example, if you select the count for AV Alert Total, you view the All Antivirus Alerts page.

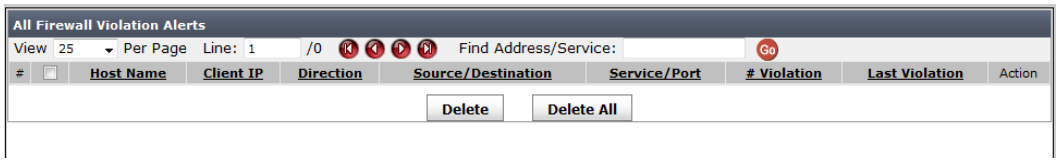
Figure 189: Client Alert Summary.



Viewing firewall alerts for FortiClient computers

In the FortiClient Manager, go to *Message Center* > *Client Alert* > *Firewall Alert* to view violations of firewall policies on your FortiClient computers.

Figure 190: All firewall alerts list.



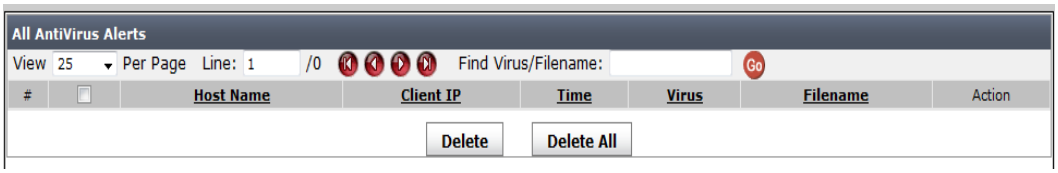
View per Page	Select the number of clients to display per page.
Line	Enter the line of the list that you want to view and select Go.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.
Find Address/Service	To find a particular IP address or firewall service in the list, enter it in this field and select Go.
#	Line numbers
Host Name	Host name of FortiClient computer.

Client IP	IP address of FortiClient computer.
Direction	Inbound or Outbound direction of violation traffic.
Source/Destination	Source (inbound) or destination (outbound) of violating traffic.
Service/Port	Firewall service in which violation occurred and the TCP or UDP port number are listed.
# Violation	The number of times this violation has occurred.
Last Violation	The time of the latest violation of this type.
Delete icon	Select to delete violation record.
Delete All	Delete all violation records.

Viewing antivirus alerts for FortiClient computers

In the FortiClient Manager, go to *Message Center* > *Client Alert* > *AntiVirus Alert* to view a list of the viruses detected on FortiClient computers.

Figure 191: All Antivirus alerts list.

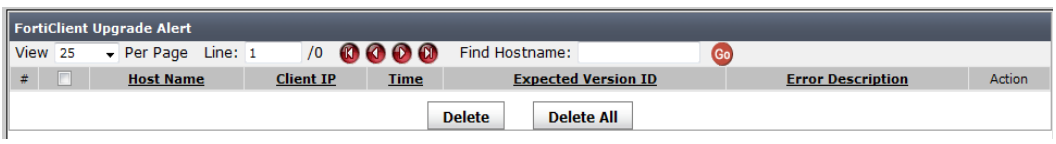


View per Page	Select the number of lines to display per page.
Line	Enter the line of the list that you want to view and select Go.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.
Find Virus/Filename	Enter the name of a virus or a file and select Go to search for it.
#	Viruses are numbered in the order they are found.
Host Name	The host where the virus was found.
Time	The time when the virus was found.
Virus	The name of the virus.
Filename	The name of the virus-infected file.
Delete	Delete the selected virus alerts.
Delete All	Delete all the virus alerts.

Viewing upgrade alerts for FortiClient computers

In the FortiClient Manager, go to *Message Center* > *Client Alert* > *Upgrade Alert* to view a list of FortiClient computers that have software upgrade problems.

Figure 192: Software Upgrade alerts list.



View per page	Select the number of lines to display per page: 25, 50, 100, or 1000
Line	Optionally, enter a line number and select Go to start the page with that line.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.
Find Hostname	Optionally, enter the host name and select Go to display only the alerts for that FortiClient computer.
#	Upgrade alerts are numbered in the order they occur.
Host Name	The host name of the affected FortiClient computer.
Client IP	The IP address of the FortiClient computer.
Time	The time of the alert.
Expected Version ID	The expected current software version on the FortiClient computer.
Error Description	Information about the upgrade alert.
Delete	Delete the selected upgrade alerts.
Delete All	Delete all the listed upgrade alerts.

Working with Clients (FortiClient computers)

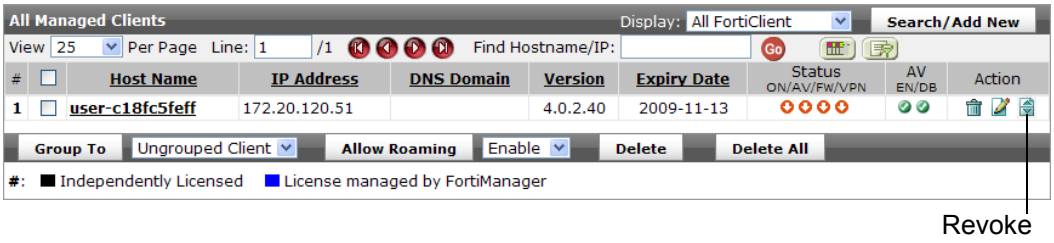
This section describes how to search, add and delete FortiClient computers. For information about configuring FortiClient computers individually or in groups, see "Configuring FortiClient computer settings" on page 343. This section includes the following topics:

Viewing the clients lists

Go to *Client/Group* > *Client* > *Managed Client* in the FortiClient Manager Navigation Pane to view the list of all managed FortiClient computers. For each computer, you can edit the description and modify the full configuration. The columns displayed depend on the Columns Display setting.

You can also set the *Display* to *Ungrouped Client* to view only the FortiClient computers that are not members of a client group.

Figure 193: All Managed Clients list.



Display	Select the group of FortiClient computers to list. By default, all FortiClient computers are listed.
Search/Add New	Find FortiClient computers on the network. This is only available when viewing the All FortiClient list. See "Searching for FortiClient computers" on page 315.
View per Page	Select the number of clients to display per page.
Line	Enter the line of the list that you want to view and press Enter.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.
Find Hostname/IP	To find a particular FortiClient computer in the list, enter the host name or IP address and select Go.
Columns Display	Select the which columns to display in this list. You can also restore the default set of columns.
Columns Filter	Apply filters to display a subset of managed clients. See "Filtering the clients list" on page 314.
#	Line number. The number is black if the FortiClient computer has a Standard Fixed license, blue if it has an Enterprise license.

The *Columns Display* setting determines which of the following columns are displayed.

Host Name	FortiClient computer host name. You can select the host name to access configuration settings for the FortiClient computer.
IP Address	IP address of FortiClient computer.
OS	Operating system of FortiClient computer.
DNS Domain	DNS domain name of FortiClient computer.
Windows Workgroup	Windows domain or workgroup of FortiClient computer.
Serial No	Serial number of FortiClient computer.
Version	FortiClient software version of FortiClient computer.
Expiry Date	License expiry date of FortiClient computer.
Last AV Update Check	Time of last check for updated AV signatures.
Status	Status indicators for Online, Antivirus, Firewall, VPN. Green up arrow indicates up/operational. Red down arrow indicates not operational.
AV Update Status	Status indicators for Antivirus engine and database.
Roaming	A checkmark indicates that Roaming is enabled for this client.
Membership	The client group to which the FortiClient computer belongs.
Action	
Delete icon	Delete the FortiClient computer from the database.

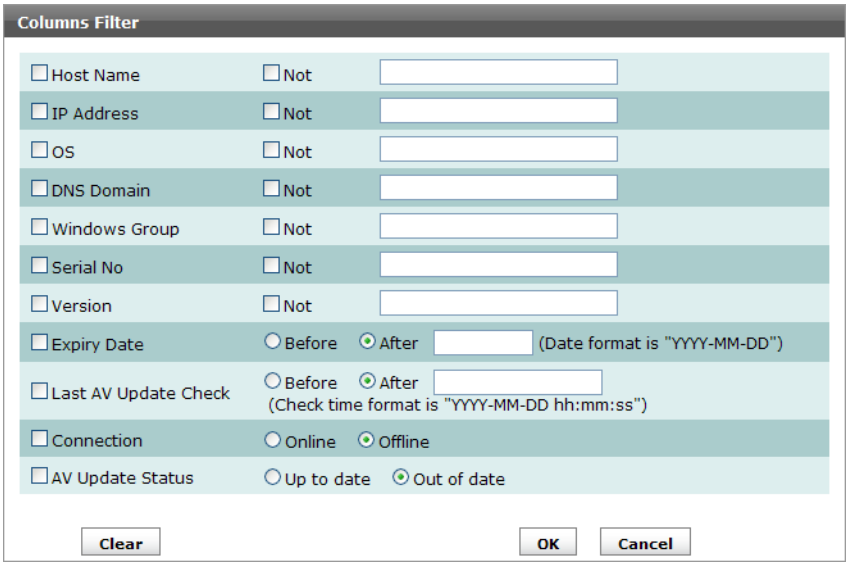
Edit icon	Edit the description for FortiClient computer.
Revoke icon	Revoke the enterprise client license of this FortiClient computer and move the FortiClient computer to the Unlicensed Clients list. See “Removing or relicensing unlicensed clients” on page 317.
Group To	Change the group to which the selected computers belong. Select the computers, select the group, and then select *Group To*.
Allow Roaming	Change the roaming status of the selected FortiClient computers. Roaming computers are dynamically grouped when they change IP address. FortiClient Manager sends the new group configuration to the FortiClient computer. Select computers, select *Enable* or *Disable*, and then select *Allow Roaming*.

Filtering the clients list

When viewing the All Managed Clients or Ungrouped Clients list, you can define filters to reduce the list by including or excluding computers based on column values. For example, you could display only the FortiClient computers on a particular subnet.


The column heading displays this icon when a filter has been applied.

Figure 194: Column Filter configuration for clients list.



To filter the client list

1. In the FortiClient Manager, in the *Managed Client* list or the *Ungrouped Client* list, select the *Columns Filter* icon.

   The *Columns Filter* dialog opens.
2. Select the column(s) that you want to filter and enter the criteria for inclusion in the list.
3. Select *OK*.

To turn off column filtering

1. In the FortiClient Manager, in the *Managed Client* list or the *Ungrouped Client* list, select the *Columns Filter* button.

   The *Columns Filter* dialog opens.

2 Clear the check box of each column you no longer want to filter, or select *Clear* to end all column filtering.

3 Select *OK*.

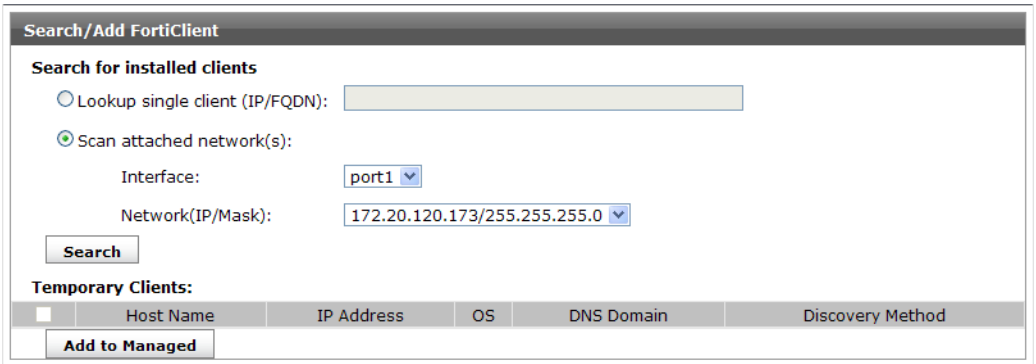
Searching for FortiClient computers

To add FortiClient computers to the FortiManager unit database, you must search the network for computers running FortiClient software. You can search for a single computer or multiple computers in the network.

If in FortiClient Manager *Settings* > *System* > *System Setting* you selected *Auto-populate managed client list*, the discovered FortiClient computers are added to the FortiManager unit as managed clients. Otherwise, the discovered clients appear in the Temporary Clients list. See "Client Discovery" in "Configuring FortiClient Manager system settings" on page 330. You can view the temporary clients and add them to the FortiManager unit at any time.

By default, FortiClient Manager adds discovered FortiClient computers to the Ungrouped Client list. If you selected the *Add to temporary clients list* option in the *Client Discovery* settings, FortiClient Manager adds discovered FortiClient computers to the Temporary Clients list. You cannot configure temporary clients until you add them to the list of managed clients. See "Adding or removing temporary clients" on page 316.

Figure 195: FortiClient search.



To search and add FortiClient computers

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client*.

2 In the All Managed Clients list, select *Search/Add New*.

3 To search a single computer, select *Lookup single client (IP/FQDN)* and enter the computer's IP address or FQDN.

4 To search multiple computers, select *Scan attached network(s)*.

- Select the *Interface* through which the FortiManager unit is connected to the network(s).
- Select the *Network (IP/Mask)* from which you want to search for FortiClient computers.

5 Select *Search*.

The discovered computers are listed with hostnames and IP addresses.

6 To add the discovered computers to the FortiManager unit, do one of the following and select *Add to Managed*:

- To add all discovered computers, select the check box at the top.
- To add a single discovered computer, select the check box before the computer in the list.

If *Auto-populate managed client list* is enabled in FortiClient global settings, the discovered computers are automatically added to the database and the *Add to Managed* button is not available.

To view and add temporary FortiClient computers

1 In the FortiClient Manager, select *Client Group* > *Client* > *Temporary Client*.

2 To add listed computers to the FortiManager unit, do one of the following and select *Add to Managed*:

- To add all discovered computers, select the check box at the top.
- To add a single discovered computer, select the check box before the computer in the list.

3 To remove computers from the temporary FortiClient computer list, do one of the following and select *Delete*:

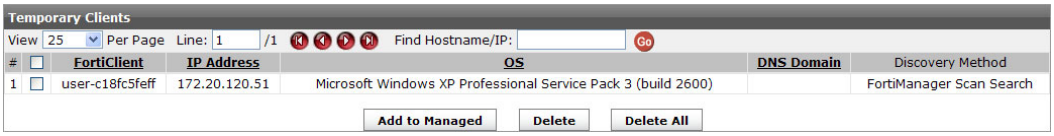
- To delete all computers, select the check box at the top.
- To delete a single computer, select the check box before the computer in the list.

Adding or removing temporary clients

Newly-discovered FortiClient computers are listed in the Temporary Clients list if you selected the Add to the temporary clients list option in FortiClient Manager system settings. (See “Client Discovery” in “Configuring FortiClient Manager system settings” on page 330.)

You can add temporary clients to the managed clients list or delete them.

Figure 196: Temporary clients.



View per page	Select the number of lines to display per page: 25, 50, 100, or 1000
Line	Optionally, enter a line number and select Go to start the page with that line.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.
Find Hostname/IP	Optionally, enter the host name and select Go to display only that client.
#	Temporary clients are numbered.
FortiClient	Host name of the FortiClient computer.
IP Address	IP address of the FortiClient computer.
OS	Operating system of the FortiClient computer.

DNS Domain	DNS/domain name of the FortiClient computer.
Discovery Method	The method used to discover the FortiClient computer. One of: **FortiClient Register** — FortiClient computer registered directly **FortiManager Scan Search** — FortiManager searched the network **FortiClient Query** — FortiClient computer sent discovery query on network **FortiManager Lookup Client** — FortiManager searched the network with a single client IP address
Add to Managed	Move the selected FortiClient computer to the Ungrouped Clients list.
Delete	Remove the selected FortiClient computer from the Temporary Clients list.
Delete All	Remove all FortiClient computers from the Temporary Clients list.

To add temporary FortiClient computers

1. In the FortiClient Manager, select *Client/Group* > *Client* > *Temporary Client*.
2. Select the computers you want to add.
3. Select *Add to Managed*.

   The FortiClient computers are added to the All Managed Clients and Ungrouped Clients lists.

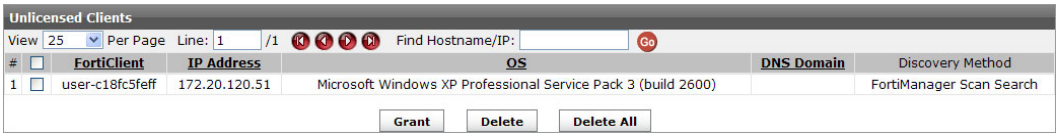
To delete temporary FortiClient computers

1. In the FortiClient Manager, select *Client/Group* > *Client* > *Temporary Client*.
2. Select the computers you want to remove
3. Select *Delete*.

Removing or relicensing unlicensed clients

If you are using Enterprise redistributable licensing and you revoked a client's license, that client is listed in the Unlicensed Client list. Go to *Client/Group* > *Client* > *Unlicensed Client* to view the list of unlicensed clients.

Figure 197: Unlicensed client list.



View per page	Select the number of lines to display per page: 25, 50, 100, or 1000
Line	Optionally, enter a line number and select Go to start the page with that line.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.
Find Hostname/IP	Optionally, enter the host name and select Go to display client.
#	Temporary clients are numbered.
FortiClient	Host name of the FortiClient computer.
IP Address	IP address of the FortiClient computer.
OS	Operating system of the FortiClient computer.

DNS Domain	DNS/domain name of the FortiClient computer.
Discovery Method	The method used to discover the FortiClient computer. One of: **FortiClient Register** — FortiClient computer registered directly **FortiManager Scan Search** — FortiManager searched the network **FortiClient Query** — FortiClient computer sent discovery query on network **FortiManager Lookup Client** — FortiManager searched the network with a single client IP address
Grant	Re-grant the FortiClient computers client license.
Delete	Remove the selected FortiClient computer from the Unlicensed Clients list.
Delete All	Remove all FortiClient computers from the Unlicensed Clients list.

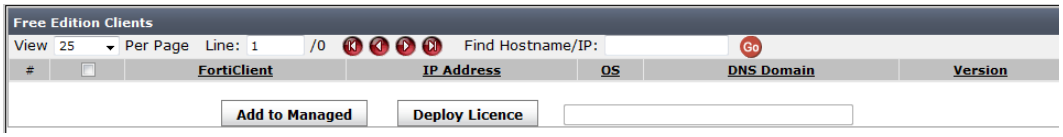
Deploying licenses to Standard (Free) Edition clients

You can view the computers running the Standard (Free) edition of FortiClient on the Free License Clients tab. The Free edition of FortiClient are those computers running FortiClient but do not have licenses. You can deploy licenses so they will be upgraded to the Premium edition. With the Premium edition, all features are “unlocked’ and the clients can be managed via FortiManager.

To deploy licenses to Free Edition clients

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Free Edition Client*.

Figure 198: Free edition client tab.



2 Select the client you want to deploy a license.

3 Enter the license number and click *Deploy License*.

Deleting FortiClient computers

You can delete FortiClient computer records from the FortiManager unit. If the computer belongs to a client group, it will be removed from the group.

To delete computers

1 In the FortiClient Manager, from the Main Menu Bar, select *Client/Group* > *Client* > *Managed Client*.

2 Select FortiClient computers from the list.

3 Select *Delete*.

Working with FortiClient groups

You may want to divide the managed FortiClient computers into groups in order to:

- Configure group-shared settings and then install the configurations on the computers all at once.
- Group FortiClient computers according to IP address, Windows Workgroup, DNS domain or operating system.

- Manage a large number of computers more efficiently.

Note: Each FortiClient computer can be added to only one group.

Overview of client groups

FortiClient Manager supports both statically and dynamically populated groups. Groups can be nested to help you organize your FortiClient computers for convenient management. A FortiClient computer can belong to only one group.

Static client group

A static group has a fixed membership that you define by selecting group members manually. When a FortiClient computer belongs to a static group, it cannot become a member of a dynamic group even if it matches the criteria.

Dynamic client group

A dynamic group has members who match one of the following criteria:

- the computer's IP address, IP address range or subnet
- the computer's DNS domain
- the operating system of the computer
- the Windows Workgroup to which the computer belongs
- the FortiClient computer's Enterprise Client License

The FortiClient Manager compares computers to the criteria of each dynamic group starting at the top of the list of groups. The computer is assigned to the first group that it matches. This dynamic grouping process runs when

- you add a new FortiClient computer to the managed list
- you edit or add a new dynamic group
- you select *Refresh* while editing a FortiClient group

Dynamic grouping applies to

- ungrouped computers
- computers that are members of dynamic groups
- computers that have roaming enabled

Nested groups

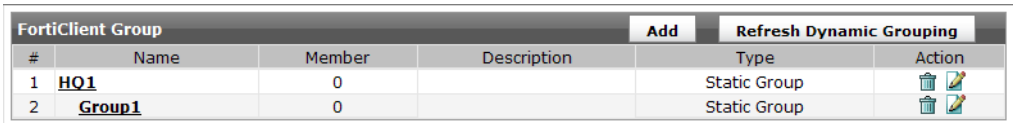
You can create groups of groups. To assign a group as a member of another group, you select that group as the parent group. For example, to make Group B a member of Group A, when you configure Group B you select Group A as the parent group.

Dynamic groups can be members of static groups and vice versa. Nesting is limited to eight levels in depth.

Viewing FortiClient groups

Select *Client/Group* > *Group* in the FortiClient Manager Navigation Pane to view the FortiClient Group list.

Figure 199: FortiClient Group list.

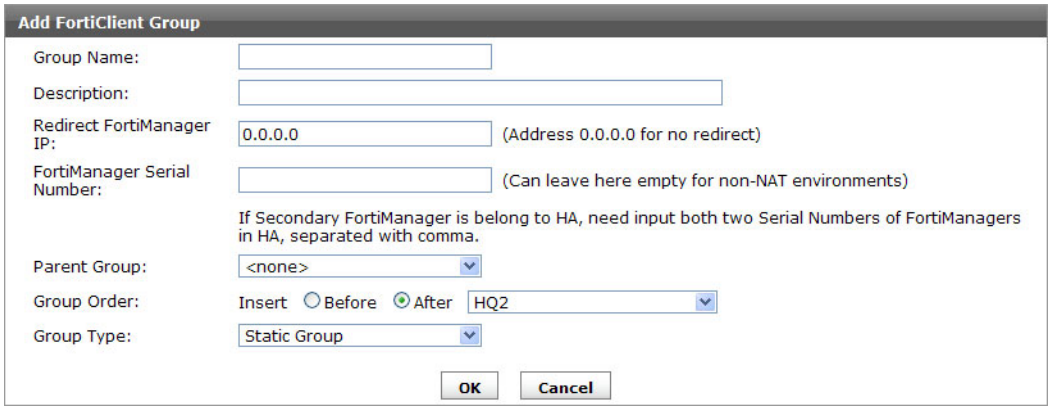


Add	Create a new FortiClient group. See "Adding a FortiClient computer group" on page 320.
Refresh Dynamic Grouping	Recreate dynamic groups based on their criteria.
Name	FortiClient group name. Select to edit FortiClient settings for the group.
Member	The number of members in the group. This does not include members of nested groups.
Description	Optional description of the group.
Type	Static or Dynamic. For more information, see "Overview of client groups" on page 319.
Action	
Delete icon	Delete this group.
Edit icon	Edit the group membership and settings. For information about fields, see "Adding a FortiClient computer group" on page 320.

Adding a FortiClient computer group

In the FortiClient Manager, to add a client group, select *Client/Group* > *Group* in the Navigation Pane and then select *Add* in the Content Pane. Enter the required information and select *OK*.

Figure 200: Add FortiClient group.



Group Name	Enter a unique *Group Name*. The name cannot be the same as the name of another computer or computer group.
Description	Enter a *Description* for the computer group. You can use the description to provide more information about the FortiClient computer group. For example, you could include its location or any other useful information.

Redirect FortiManager IP	This field is available only if clustering is enabled. In a FortiClient Manager cluster, this is the address of the FortiClient Manager where FortiClient computers in this group should log on. FortiClient computers can log on to the primary server in the cluster but are redirected to this specified secondary server. A value of 0.0.0.0 disables redirection.
FortiManager Serial Number	Enter the serial number of the FortiManager unit. This is necessary only if the FortiClient computer or the FortiManager unit is behind a NAT device. If a FortiManager cluster manages the group, enter the serial numbers of both units separated by a comma.
Parent Group	To create a nested group, select the group to which this group belongs.
Group Order	Select an existing group from the list and choose whether the new group appears before or after that group in the Navigation Pane.
Group Type	Select *Static Group* to manually group computers using the Group Members list. Select *Dynamic Group* to group computers based on the *Policy*.
Policy	For a dynamic group, select the criteria for membership in this client group. One of:
DNS domain	Type the DNS domain name or select it from the *Select* list.
Operating System	Type the operating system name or select it from the *Select* list.
Windows Workgroup	Type the Windows Workgroup name or select it from the *Select* list.
IP Range/Subnet	Enter an IP address, an IP address range such as 192.168.1.2-192.168.1.5, or a subnet address such as 192.168.1.0/24. You can specify multiple address criteria if you enter them as separate lines.
Enterprise Client License	Type the Enterprise Client License key.

You add clients to the group by using the *Group To* button in the All Managed Clients list. See "Viewing the clients lists" on page 312.

Deleting a FortiClient computer group

You can delete a single group, multiple groups, or all the groups at once. This does not delete the member devices.

To delete computer groups

1. In the FortiClient Manager, select *Client/Group* > *Group*.
2. Select the group or groups you want to delete, then select *Delete*.
3. If you want to delete all the groups, select *Delete All*.

Editing a FortiClient computer group

You can modify group description, adjust group order, and change group type.

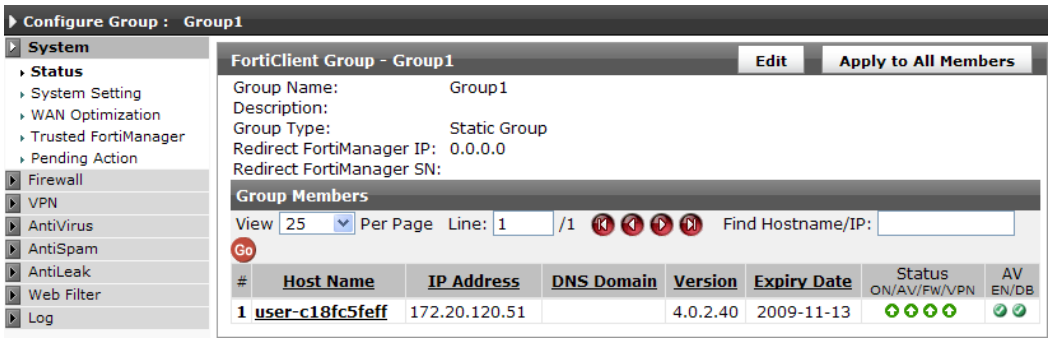
To edit a client group

1. In the FortiClient Manager, from the Navigation Pane, select *Client/Group* > *Group*.
2. Select the client group that you want to modify.
3. Select *Edit*.
4. Make the changes and select *OK*.

Viewing group summaries

In the Navigation Pane, go to *FortiClient Manager* > *Client/Group* > *Group*. In the FortiClient menu, go to *System* > *Status* to view the high level information for the group.

Figure 201: Group summary.



Edit	Edit client group configuration.
Apply to all members	Apply group settings to all members, eliminating overrides.
Group Name	The name of the FortiClient computer group.
Description	Descriptive notes about the FortiClient computer group.
Group Type	The type of FortiClient computer group: Static Group - manually selected members Dynamic Group - membership based on IP address, domain, Windows Workgroup or operating system
Redirect FortiManager IP	If clustering is enabled, this is the address of the secondary FortiClient Manager to which FortiClient computers are redirected. A value of 0.0.0.0 means that clustering or redirection is disabled. “About FortiClient Manager clustering” on page 304.
Redirect FortiManager SN	This is the serial number of the secondary FortiClient Manager to which FortiClient computers are redirected. See Redirect FortiManager IP, above.
Group Members	Member FortiClient computers in this group, including their hostnames and IP addresses.
Apply	Select to save the FortiClient computer group.

Configuring settings for client groups

You can select a FortiClient computer group and configure the settings shared by all the computers in this group, including trusted FortiManager units, firewall, VPN, antivirus, web filter, and logs.

The configuration steps are identical to configuring a single managed FortiClient computer, except that group settings apply to all members in the group and that, in most cases, there is no override function in group configurations. See “Configuring FortiClient computer settings” on page 343.

The override server configuration under Web Filter is the only override function associated with group settings. Once you select the override options and complete the configuration, the FortiClient computers will get the web filtering and anti-spam settings from the FortiManager unit instead of from the FortiGuard server through the Internet. See “Configuring web filter options on a FortiClient computer” on page 376.

After completing a configuration for a group or a member FortiClient computer configuration, you can copy the group configuration to other groups or the member FortiClient computer configuration to the group to which it belongs.

The group and member configurations that can be copied include:

- System > Trusted FMGs
- Firewall > Policies/Addresses/Service/Schedules
- VPN
- Anti Virus > Scheduled Scans

You can override specific group settings in a group member's configuration. In the group configuration you can reapply the group settings to all members.

To copy a group configuration to other groups

1. In the FortiClient Manager, go to *Client/Group* > *Group* and select a FortiClient group in the *Client/Group Tree*.
2. From the FortiClient menu, select the configuration that you want to copy, for example Firewall > IP Address.
3. From the *Action* column, select the *Copy to other group(s)* icon.
4. Select the target group(s) to which you want to copy a group configuration.
5. Select one of the options for *When same name configuration exists in export-to group(s): Overwrite* or *Keep unchanged*.
6. Select *OK*.

To reapply group settings to all members

1. In the FortiClient Manager, go to *Client/Group* > *Group* and select a FortiClient group in the Client/Group Tree.
2. From the FortiClient menu, select the configuration that you want to apply to all of the group members, for example Firewall > IP Address.
3. Do one of the following:
   - From the *Action* column, select the setting's *Apply to member(s)* icon.
   - To apply all settings on the configuration page to all group members, select *Apply to All Members* at the top of the page.
4. Select *OK* to confirm copying the configuration.

To export a member configuration to its parent group

1. In the FortiClient Manager, go to *Client/Group* > *Group* and select a FortiClient group in the Client/Group Tree.
2. In the *Group Members* list, select a member.
3. From the FortiClient menu, select the configuration that you want to copy to the group, for example Firewall > IP Address.
4. Select *Override*.
5. Select the *Copy to group* icon for the configuration that you want to export.

Managing client configurations and software

Using FortiClient Manager, you can

- deploy configurations to FortiClient computers
- retrieve configurations from newly-added FortiClient computers
- make software upgrades available to FortiClient computers
- manage the licensing of FortiClient software

Deploying FortiClient computer configurations

After you make configuration changes, you can deploy the changes to the FortiClient computers. Before you deploy them, all the changes are stored in the FortiManager database.

Note: Deployment may fail if you make configuration changes on the computer at the same time. For details, see "Retrieving a FortiClient computer configuration" on page 324.

To deploy configuration changes to client groups

1. In the FortiClient Manager, select *Manage* > *Deploy Configuration* in the Main Menu Bar.
2. Select one of these options:

   Deploy all configuration changes — Deploy changes to all affected FortiClient computers.

   Deploy configuration changes for FortiClient computers in selected groups — FortiClient computers in child groups of the selected group are not affected.

   Deploy configuration changes for FortiClient computers in selected groups and child groups — Changes are also deployed to FortiClient computers in child groups of the selected group.
3. Unless you selected *Deploy all configuration changes*, select the groups to which you want to deploy the changes.
4. Select *Deploy*.

To deploy configuration changes to individual FortiClient computers

1. In the FortiClient Manager, select *Manage* > *Deploy Configuration* in the Main Menu Bar.
2. Select the *Deploy Configuration to Client* tab.
3. Select the FortiClient computers to which you want to deploy the updated configuration.

   If you select the check box in the table heading, all FortiClient computers are selected.
4. Select *Deploy*.

Retrieving a FortiClient computer configuration

After you add a FortiClient computer to the FortiManager system, you can resynchronize with the computer by retrieving the FortiClient configuration from the computer and saving it to the FortiManager database.

After resynchronization, if you make any FortiClient configuration changes on the computer rather than through the FortiManager System, the configuration on the computer and the configuration saved in the FortiManager database will be out of sync. In this case, you can resync the computer again.

The installation of configuration changes to a computer may fail if you make configuration changes on the computer at the same time.

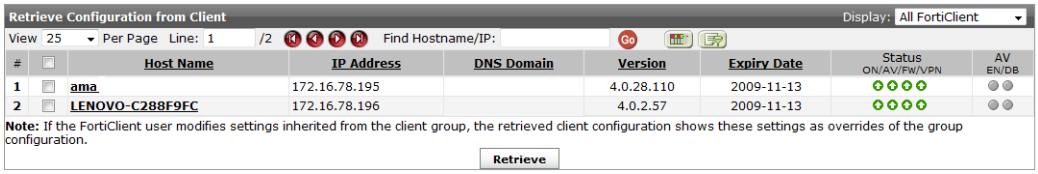
To resynchronize a computer

1 In the FortiClient Manager, select *Manage* > *Retrieve Configuration* in the Main Menu Bar.

2 Select the computer(s) that you want to resync, then select *Retrieve*.

The resync process may take a few minutes, depending on network speed.

Figure 202: Retrieving a configuration from a client.

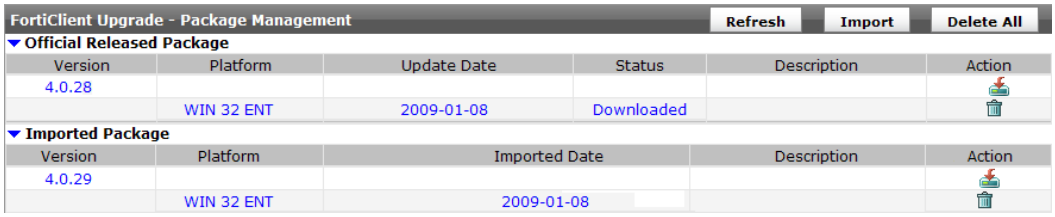


Working with FortiClient software upgrades

The FortiManager unit can update FortiClient application installations with software updates retrieved from the FortiGuard service. In the FortiClient Manager, go to *Manage* > *FortiClient Upgrade* to view the available upgrade packages.

Note: FortiManager cannot update FortiClient software older than version 3.0 MR6 (Build 534).

Figure 203: List of available FortiClient software upgrades.



Delete All	Delete all of the listed upgrade packages.
Refresh	Update the list.
Import	Manually import a software package. This is used to add customized FortiClient installation packages to the *Imported Package* list. For more information, see “Importing a software upgrade package” on page 326.
Version	The major version and build number. For example, 3.0.521 is version 3.0 build 521.
Platform	One of: WIN 32 ENT - Windows 32-bit Enterprise edition WIN 64 ENT - Windows 64-bit Enterprise edition
Date	The date and time when the software upgrade was released.
Status	For official released packages only. One of: Ready - the software upgrade is ready to download from FDS. Accept - download requested Processing - FortiClient Manager is downloading the software upgrade Downloaded - imported software upgrade is ready to deploy Failed - download of software upgrade failed

Description	A description of the package.
Action	Download - download the software upgrade Deploy - deploy software upgrade to clients Delete - delete the upgrade package

Importing a software upgrade package

You can add customized FortiClient installation packages to the software upgrades list.

To import a package

1. In the FortiClient Manager, go to *Manage* > *FortiClient Upgrade* and select Import.
2. Enter the *Version*, 4.0.3, for example.
3. Enter a *Description* of the package.

   This is important if you provide multiple custom installer packages.
4. From the *Platform* list, select the appropriate operating system type (32-bit or 64-bit Windows) for the package you will upload.
5. Select *Browse*, find the customized FortiClient installation file, and select *Open*.
6. Select *OK*.

   The file is uploaded and added to the FortiClient Software Upgrade list.

Deploying a software upgrade to clients

When you have downloaded FortiClient software upgrades to the FortiManager unit (see "Working with FortiClient software upgrades"), you can then deploy them to FortiClient computers.

To deploy software upgrades to FortiClient computers

1. In the FortiClient Manager, select *Manage* > *FortiClient Upgrade* from the Main Menu Bar.
2. Select the *Deploy* icon for the software upgrade that you want to deploy.
3. Select whether to deploy the software to groups or to individual FortiClient computers. The options are
   - selected group(s)
   - selected group(s) and child group(s)
   - selected FortiClient computer(s)
4. Enable *Select All* or select the particular groups or computers to receive the software upgrade.
5. Select *Apply*.

If an error occurs when upgrading a FortiClient computer's software, an alert is raised. See "Viewing upgrade alerts for FortiClient computers" on page 311.

FortiClient license keys

You can assign and deploy Premium (Volume) license keys to client groups. In the FortiClient Manager, go to *Manage* > *FortiClient Key* to view the current list of assigned license keys.

Note: The FortiClient License Key Management page does not handle enterprise redistributable licensing. For information about using enterprise licensing, see "Configuring enterprise license management" on page 340.

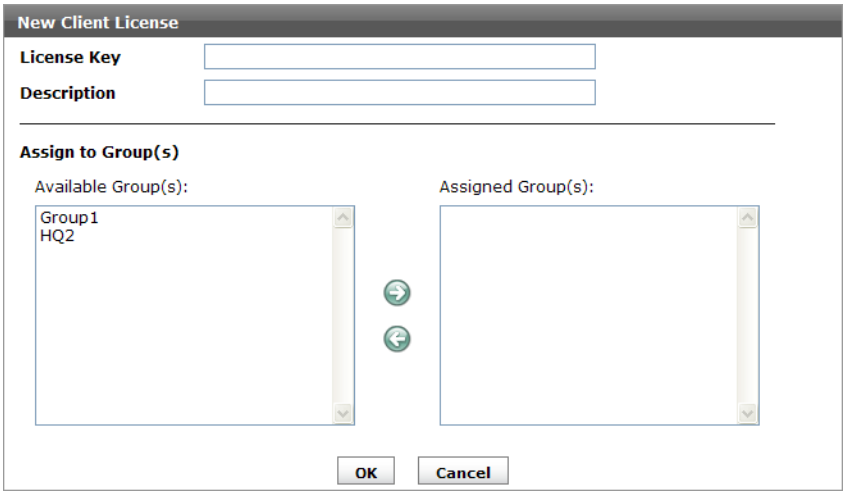
There are several ways to apply Premium (Volume) licensing:

- Provide the license key to your users to enter directly into the FortiClient application. The license will by managed by FDS, not by FortiManager.
- Create a customized FortiClient installer that includes the license key. Distribute the customized FortiClient installer to your users. Use the “-a”, and “-k” switches in the FCRepackager tool . For more information, see the *FortiClient Administration Guide*.
- If you manage FortiClient computer with a FortiManager unit, you can deploy the licenses. See “To deploy Premium (Volume) license with FortiManager”. The license is applied to all of your managed FortiClient computers that already do not have a Premium license. The volume license has a seat limit which the FortiManager unit enforces.

To deploy Premium (Volume) license with FortiManager

1. Using FortiClient Manager, organize the managed FortiClient computer into client groups where all members use the same license key.
2. In the FortiClient Manager, go to *Manage* > *FortiClient Key* and select *Add* to add a license key to the FortiManager database.

Figure 204: Adding a FortiClient license key.



3. In the *License Key* field, enter the license key.
4. Optionally, enter a description.
5. In the *Available Group(s)* list, select the client groups that use this license key and then select the green right arrow button to move the selected groups to the *Assigned Group(s)* list.
6. Click *OK*.
7. In the FortiClient *License Key Management* list, select the *Deploy to group* icon for the license key that you added. Click *OK* to confirm your request to deploy.

Working with web filter profiles

You can create web filter profiles in FortiManager and deploy them to FortiClient computers, FortiClient groups, Windows AD users, and Windows AD groups.

To assign web filter profiles to FortiClient computers and groups, see “Selecting a web filter profile for a FortiClient computer” on page 375.

To assign web filter profiles to Windows network users and groups, see “Working with Windows AD users and groups” on page 335.

About web filtering

FortiGuard Web Filtering is a managed web filtering solution provided by Fortinet. FortiGuard Web Filtering sorts hundreds of millions of web pages into a wide range of categories that users can allow, block, or monitor.

FortiGuard Web Filtering can also assign one of several classifications to denote web sites that provide cached content, such as web site search engines, or web sites that allow image, audio, or video searches.

The FortiClient computer accesses the nearest FortiGuard Web Service Point to determine the categories and classification of a requested web page. The FortiClient application blocks the web page if the web page is in a category or classification that is blocked in the assigned web profile.

There three predefined profiles to allow or block different combinations of web categories:

Default	Default web filter profile, which is initially the same as the Child profile.
Child	Blocks categories that are not suitable for children.
Adult	Only blocks the security violating web sites.

You cannot delete the predefined profiles, but you can modify them. You can also create additional web profiles as needed.

You can assign web profiles to FortiClient computers and FortiClient groups. On a Windows AD network, you can also assign web profiles to each network user. FortiClient Manager sends the user’s web filter information to the FortiClient computer where the user is logged on.

Viewing and editing web filter profiles

In the FortiClient Manager, go to *Global Configuration* > *Web Filter Profile* to manage web filter profiles.

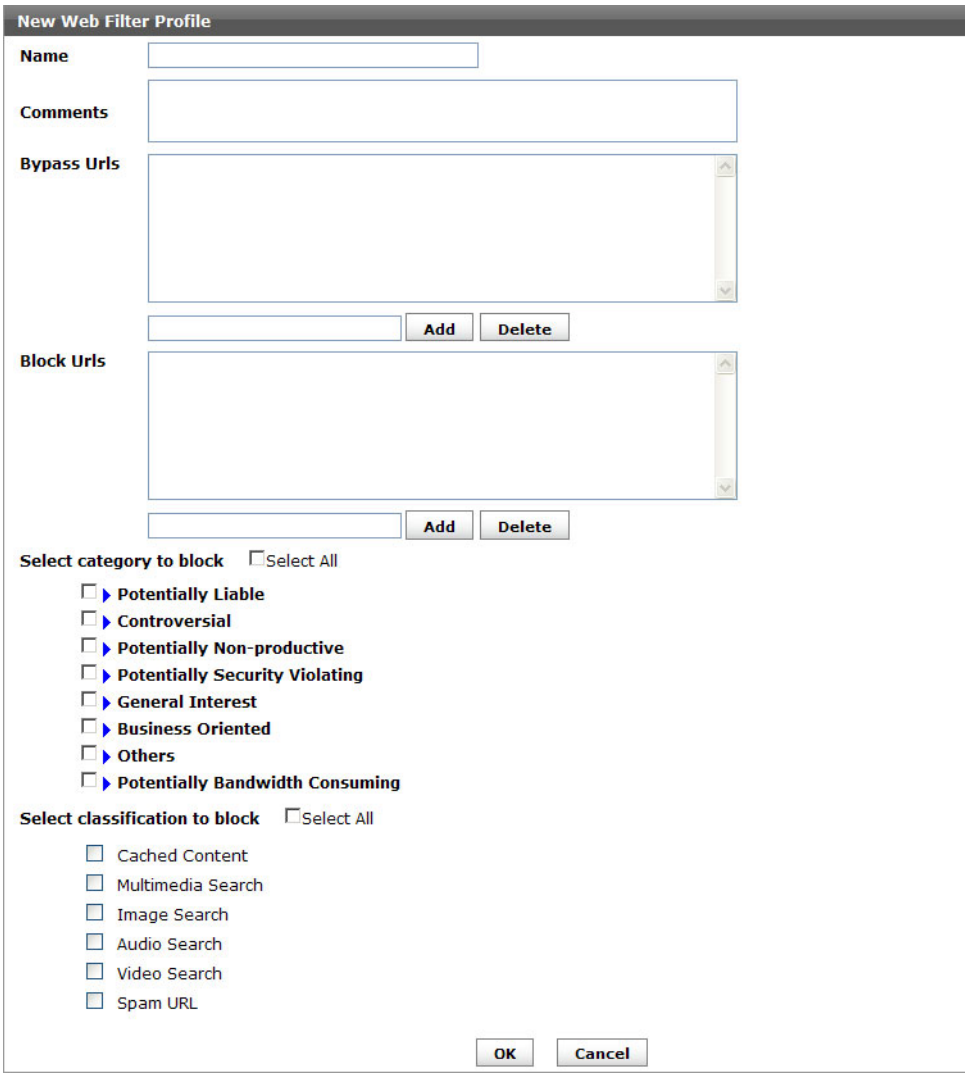
Figure 205: Web Filter Profiles.

Create New	Create a new web filter profile. See “Configuring a web filter profile” on page 329.
Name	The profile name
Comments	A description or comment about the profile
Action	
Delete icon	Delete this profile. You cannot delete the predefined Default, Child or Adult profiles.
Edit icon	Edit this profile.

Configuring a web filter profile

In the FortiClient Manager, go to *Global Configuration* > *Web Filter Profile*. Select *Create New* to create a new profile or select the *Edit* icon of an existing profile to modify the profile.

Figure 206: Configuring a web filter profile.



Enter the following information and select *OK*.

Name	Enter a name for the profile.
Comments	Optionally, enter descriptive information about the profile.
Bypass URLs **Block URLs**	Bypass URLs are allowed even if they are in a blocked category. Block URLs are always blocked. To add a URL, enter it in the field below the list and select *Add*. To remove a URL, select it in the list and then select *Delete*.
Select category to block	Either select *Select All* or select individual categories to block. You can expand the categories to select specific sub-categories.
Select classification to block	Either select *Select All* or select individual classifications to block.

Configuring FortiClient Manager system settings

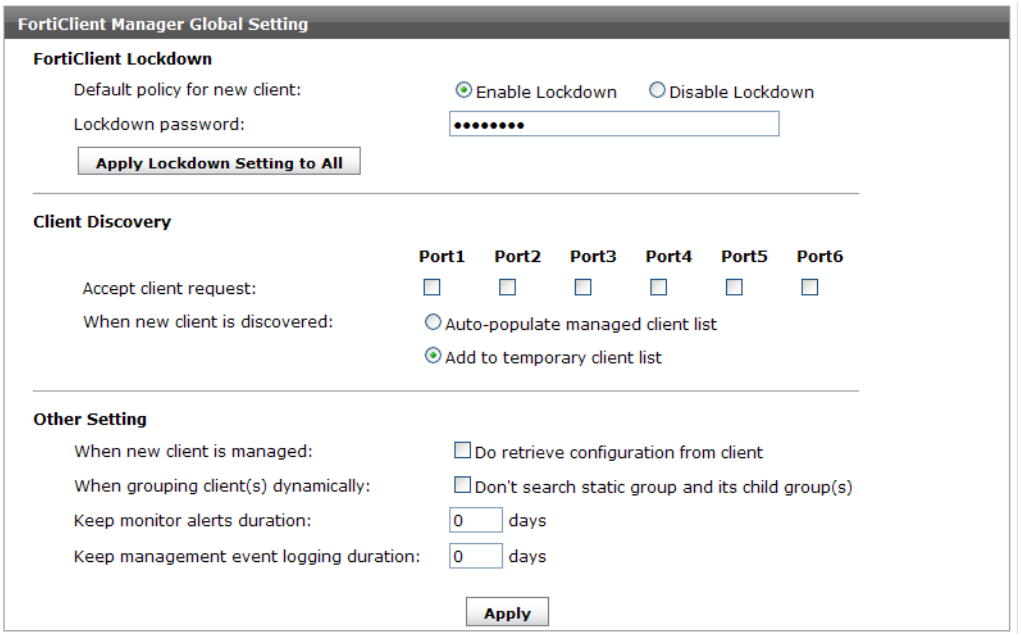
The FortiClient Manager system settings include:

- FortiClient configuration lockdown settings
- FortiClient computer discovery settings

FortiClient group administrators can only view these settings. For more information about group administrators, see "Configuring FortiClient group-based administration" on page 339.

In the FortiClient Manager, go to *Settings* > *System* > *System Setting*. Enter the following information and then select *Apply*.

Figure 207: FortiClient Manager global settings.



FortiClient Lockdown

You can lock the configuration of FortiClient computers. Users cannot remove the software and cannot change the settings. Users can connect and disconnect VPN tunnels and can change certificates and CRLs.

You can override the lockdown setting on groups or individual FortiClient computers. See "Configuring system settings of a FortiClient computer" on page 345.

Default policy for new client

Select *Enable Lockdown* or *Disable Lockdown*.

Lockdown password

Enter a password. You can provide this password to users to enable them to modify their own configuration, using FortiClient override. For information on the FortiClient override feature, see *FortiClient Endpoint Security User Guide*.

Apply Lockdown Setting to All

Apply the lockdown settings to all FortiClient computers that this FortiManager unit manages.

Client Discovery

Accept client request

Select the network interfaces (ports) on which the FortiManager unit listens for registration requests, either broadcast or unicast, from FortiClient computers.

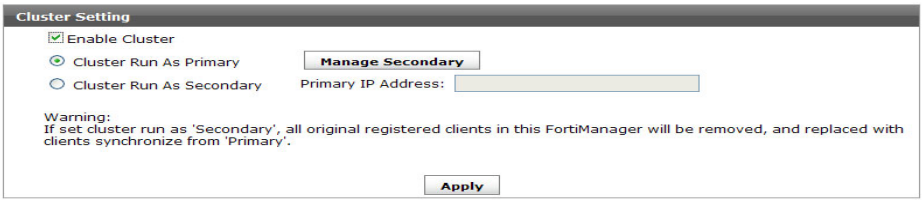
When new client is discovered	Select *Auto-populate managed client list* if you want newly-discovered FortiClient computers added to the Managed Client and Ungrouped Client lists in the Navigation Pane. Otherwise, select *Add to temporary client list*.
Other Setting	
Do retrieve configuration from client	Select to retrieve the configuration from a new client when it is added to the managed clients list.
Don't search static group and its child group(s)	Enable only to speed up dynamic grouping where there are no static groups with dynamic child groups. The default is to not enable this option.
Keep monitor alerts duration	Enter the time that firewall and antivirus alerts are retained before automatic deletion. Enter 0 to keep alerts until you manually delete them.
Keep management Event Logging duration	Enter the number of days to retain management event logs.

Configuring FortiClient Manager clustering

Clustering enables you to support a large number of FortiClient computers by using multiple FortiManager units. One FortiManager unit must be declared as the primary unit. The others are all secondary units. For more information, see “About FortiClient Manager clustering” on page 304.

In the FortiClient Manager, go to *Settings* > *System* > *Cluster Setting* to configure FortiClient Manager clustering.

Figure 208: FortiClient Manager cluster settings.



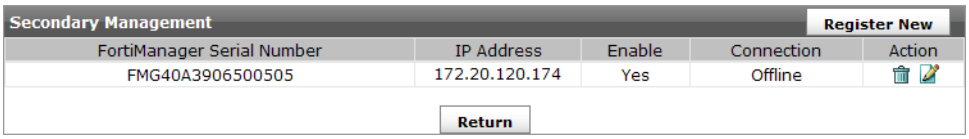
Enable cluster	Select to enable clustering and then enable one of the following options.
Cluster Run as Primary	Enable if this FortiManager is the primary unit. Select *Manage Secondary* to register secondary units. See “Configuring FortiClient Manager cluster members” on page 331.
Cluster Run as Secondary	Enable if this FortiManager is a secondary unit. Enter address of the primary unit in the *Primary IP Address* field.

Configuring FortiClient Manager cluster members

If you enable FortiClient Manager clustering and you set this FortiManager unit as the primary unit, you must register the other FortiManager units that are permitted to connect as secondary cluster members.

In the FortiClient Manager, go to *Settings* > *System* > *Cluster Setting* and select *Manage Secondary* to view or modify the list of secondary FortiManager units. Select *Return* when you are finished.

Figure 209: FortiClient Manager cluster configuration.



Register New	Select to add another secondary unit to the cluster. Enter the secondary FortiManager unit serial number and IP Address and then select *OK*. **Note:** If the secondary FortiManager is an HA cluster, enter the serial numbers of both units, separated by a comma.
FortiManager serial number	The serial number(s) of the secondary unit(s). You can find this information on the each secondary unit's *System Settings* > *General* page.
IP Address	The secondary unit's IP Address.
Enable	*Yes* or *No*
Connection	*Online* or *Offline*
Action	
Delete icon	Remove secondary unit from cluster.
Edit icon	Edit the secondary unit's information.

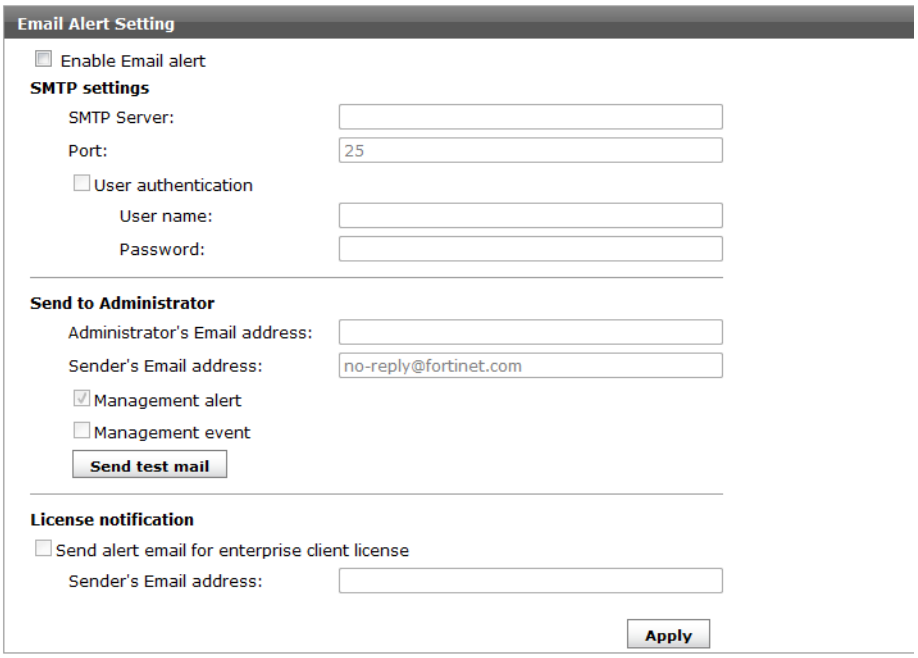
Configuring email alerts

You can configure FortiClient Manager to send email messages to administrators, or other parties, when there are management alerts or management events.

The FortiClient Manager sends an alert email message each day that there is a new alert or event. The email message contains all existing management alerts, and the total count of alerts. Optionally, the message can also contain the latest management events and total count of existing events.

In FortiClient Manager, go to *Settings* > *System* > *Email Alert Setting* to configure email alerts. Enter the following information and select *Apply*.

Figure 210: FortiClient Manager email alert settings.



Enable Email alert	Send email alerts using the account and content settings below.
Email Account	
SMTP Server	Enter the SMTP mail server IP address or fully qualified domain name.
Port	Enter the port number that the mail server uses. The default is 25.
User authentication	Select if the mail server requires authentication, then enter the *Username* and *Password* of the sending email account.
Send to Administrator	
Administrator's Email address	Enter the email address of the person who will receive alerts.
Sender's Email address	Enter the reply-to address to provide in alert email messages.
Management Alert	Select if this email is in regards to a management alert.
Management Event	Select if this email is in regards to a management event.
Send test mail	Send a test email using the *Email Account* settings.
License notification	
Send alert email for enterprise client license	Select if the email is to notify to user of the FortiClient license.
Sender's email address	Enter the email address.

Configuring LDAP for web filtering

The FortiManager system can provide individualized web filter settings for users and groups on a Microsoft® Windows Active Directory network. A user can log on at any computer in the network. The FortiClient application on that computer requests web filter settings for that user from FortiManager.

In the FortiClient Manager, you assign web filter profiles to Active Directory (AD) groups and users. Users to which you have not assigned a profile are assigned to a default profile.

Configuring LDAP settings

FortiClient Manager uses LDAP protocol to retrieve information about Windows Active Directory users and groups from the domain controller.

In the FortiClient Manager, go to *Settings* > *LDAP Group/User* > *LDAP Settings* to view the list of LDAP servers.

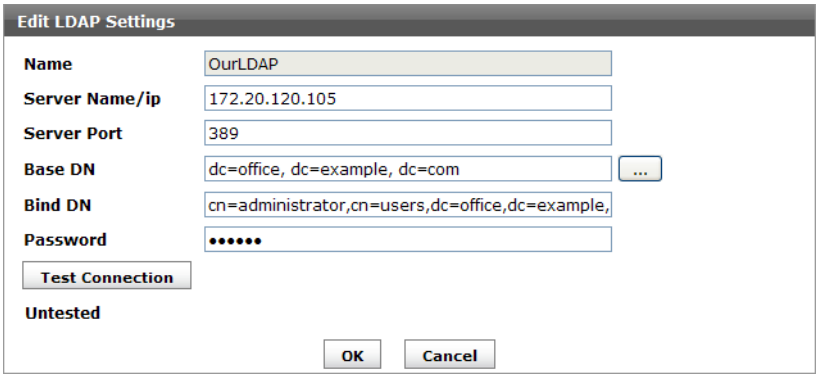
Figure 211: List of LDAP servers.

Create New	Add another LDAP server. See "Configuring an LDAP server" on page 334.
Name	The name of the LDAP server.
LDAP Server	The server IP address and port of the Windows AD domain controller.
BaseDN	The Base Distinguished Name for the server. This describes what portion of the users and groups are in this server's database.
BindDN	The Distinguished Name the FortiManager must use to log on to the LDAP server to make queries. (Maximum 255 characters)
Action	
Delete icon	Delete this entry.
Edit icon	Modify the settings for this LDAP server. See "Configuring an LDAP server" on page 334.

Configuring an LDAP server

In the FortiClient Manager, go to *Settings* > *LDAP Group/User* > *LDAP Settings* and select *Create New* to add an LDAP server. You can also select the *Edit* icon for an LDAP server on the LDAP Settings page to modify the settings for an existing server.

Figure 212: LDAP server settings.



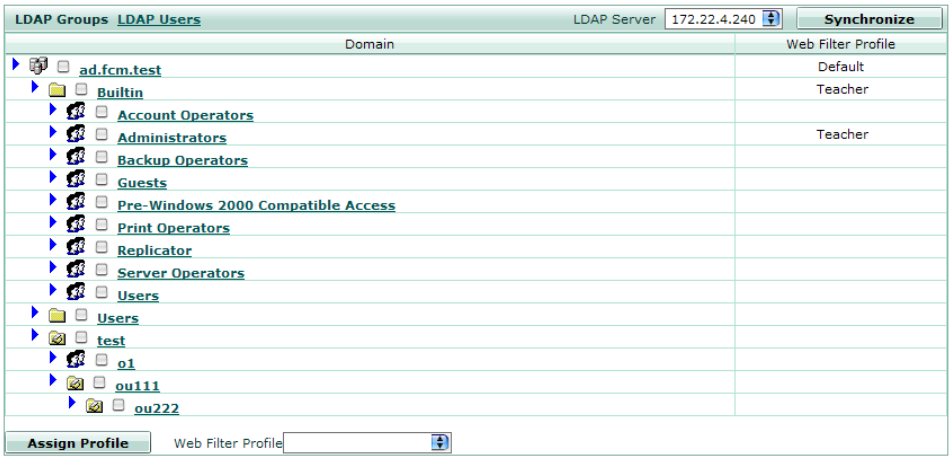
Enter the following information and select OK.

Name	Enter a name for this LDAP server.
Server Name/IP	Enter the fully-qualified domain name or IP address of the Windows AD domain controller.
Server Port	Enter the port used to communicate with the LDAP server. The default is port 389. If needed, change the port to match the server.
BaseDN	Enter the Base Distinguished Name for the server. You can get this information from the server's administrator.
BindDN	Enter the Bind Distinguished Name for the server. You can get this information from the server's administrator.
Password	Enter the password required for logon to make queries.
Test Connection	Attempt to connect to LDAP server as configured. Results display below button.

Working with Windows AD users and groups

In the FortiClient Manager, go to *Settings* > *LDAP Group/User* > *LDAP Group/User* to view a list of Windows Active Directory (AD) domains, groups and users. You can assign web filter profiles to groups and users.

Figure 213: List of Windows AD domains and groups.

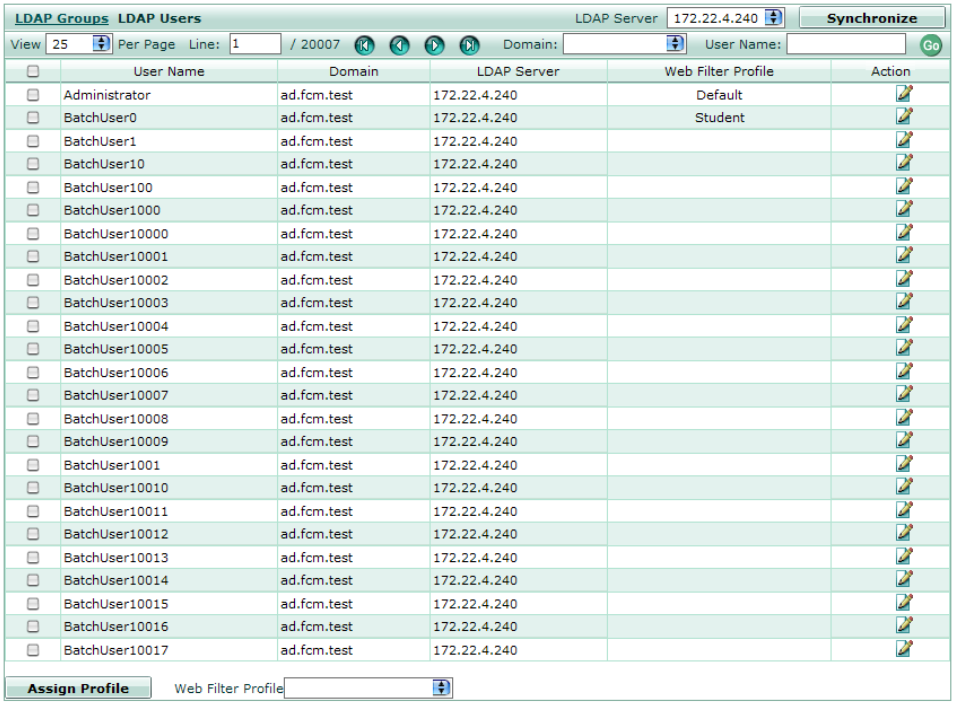


LDAP Groups view

LDAP Users	Switch to LDAP Users view.

LDAP Server	Select the Windows Active Directory (AD) domain controller.
Synchronize	Update displayed group information from Windows AD server.
Domain	Windows AD domain. Expand domains to show groups. Each group names is preceded by a check box that you can use to select the group when assigning profiles. Select the group name to view group members.
Web Filter Profile	The web filter profile assigned to this group. To configure web filter profiles, see "Working with web filter profiles" on page 327.
Assign Profile / Web Filter Profile	Select a profile from the *Web Filter Profile* list and then select *Assign Profile* to assign it to the selected groups.

Figure 214: List of Windows Active Directory users.



LDAP Users view

LDAP Groups	Switch to LDAP Groups view.
LDAP Server	Select the Windows AD domain controller.
Synchronize	Update displayed user information from Windows AD server.
View	Select the number of users to list per page.
Line	Select the line of the list you want to view and press Enter.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.
Domain	Windows AD domain. Expand domains to show groups. Each group names is preceded by a check box that you can use to select the group when assigning profiles.

User Name / Go button	Find a name in the list. Enter the name and select Go.
Check box	Use the check box to select the user for web filter profile assignment. The check box in the table heading selects all users.
User Name	User name retrieved from Windows AD
Domain	Windows AD domain name
LDAP Server	Windows AD domain controller
Web Filter Profile	The web filter profile assigned to this user. To configure web filter profiles, see "Working with web filter profiles" on page 327.
Action	*Edit* icon - View information about this user.
Assign Profile / Web Filter Profile	Assign the profile selected in Web Filter Profile list to the selected users.

Active Directory Organizational Units Grouping

In a Microsoft® Windows server environment, a useful type of directory object contained within domains is the organizational unit. Organizational units (OU) are Active Directory (AD) containers into which you can place users, groups, computers, and other organizational units. An organizational unit cannot contain objects from other domains.

FortiClient Manager allows for AD OU grouping in order to easily manage FortiClient/AD OU groups. After you synchronize the AD server to FortiClient Manager, all the AD OUs are imported into into FortiClient Manager. You can then keep all the policies set on a FortiClient group up to date, even when new FortiClient users are added to AD OUs.

After a new user is added to a AD OU group and FortiClient is installed on the user's computer, FortiClient automatically registers with FortiClient Manager. Then FortiClient Manager automatically places the new user into the correct group based on the computer's domain and computer name. After registration, FortiClient Manger sends the policies for the group the new user was placed in.

To add Active Directory Organizational Unit to FortiClient Manager groups

1. Create the LDAP (Active Directory) server settings that will use the Organizational Units (OU). Go to *FortiClient Manager* > *Settings* > *LDAP Integration* > *LDAP Settings* and click *Create New*.
2. Configure the LDAP server settings. See "Configuring LDAP settings" on page 334.
3. Create the OU group. Go to *FortiClient Manager* > *Settings* > *LDAP Integration* > *AD OU Grouping* and click *Create New*.
4. In the *New AD Grouping* window enter the following information:

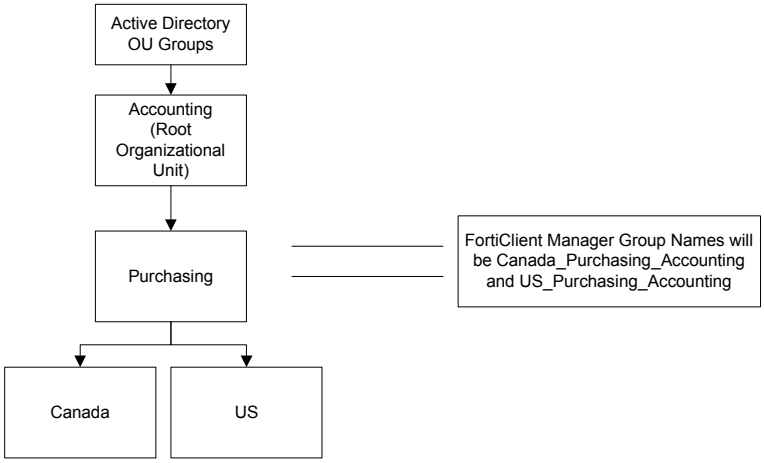
Name	Enter a name for the AD OU grouping.
LDAP Name	Select the name of the LDAP server created in Step 1.
Root OU	Select the OU group level. You can select any OU as the root OU. All OUs under the root OU will be imported into the FortiClient groups.
Description	Enter a description for the OU group.

5. Sychronize the AD OU and FortiClient. In the AD OU Grouping tab, click the *Sychronizing with AD Server* icon  .

6 Once the synchronizing is complete, you can view the AD OU groups. Go to *FortiClient Manager* > *Client/Group* > *Group*. The OU groups are displayed in the tree.

The imported FortiClient group names consist of the names of each level in the OU starting from the Root OU. For example, if the Root OU is Accounting and the subsequent level is Purchasing, and then Canada and US at the same level, then the FortiClient group names will be Canada_Purchasing_Accounting and US_Purchasing_Accounting.

Figure 215: Example of how FortiClient Manager determines the group names for OU groups.



If an OU is deleted from the AD server, a delete icon is displayed on the group name in the tree and the word (Deleted) shown next to the group name to indicate that it has been deleted from the AD server. The FortiClient group name will remain in the list. You can copy its policy to another group and/or delete it from FortiClient Manager permanently.

7 Select the OU group from the tree to configure policies and browse FortiClient users. See “Configuring FortiClient computer settings” on page 343.

Synchronizing the AD server with FortiClient Manager

You can set the amount of time that FortiClient Manager automatically synchronizes with the Active Directory (AD) server to import any new or changed Organizational Units (OU) groups. The default time is 10 minutes.

After any new or changed OU groups are imported into FortiClient Manager and after FortiClient registers, FortiClient Manager matches the host name and domain name in the tree structure and puts it into the correct OU group. The policies on the OU group will be automatically pushed out to the new or changed clients.

To set the synchronize time

1 Go to *FortiClient Manager* > *Settings* > *LDAP Integration* > *AD OU Grouping*.

2 Click *Settings*.

3 In the AD Group Settings tab, enter the number of minutes to synchronize the AD server with FortiClient Manager.

4 Click *Apply*.

Viewing the AD Grouping History

In the Active Directory (AD) Grouping History, you can see the Organizational Units (OUs) that have been added, deleted and the FortiClient group it belongs to when the AD server is synchronized with FortiClient Manager.

To view the AD Grouping history

1. Go to *FortiClient Manager* > *Settings* > *LDAP Integration* > *AD OU Grouping*.
2. Click the *AD Grouping History* link.
3. In the *AD Grouping History* tab, you can search, delete or delete all the history.

Configuring FortiClient group-based administration

You can divide administration of FortiClient computer groups among several group administrators. A group administrator is assigned particular FortiClient groups and optionally also has access to ungrouped clients. With the assigned FortiClient computers, the group administrator can

- monitor status
- retrieve, modify and deploy configurations
- change group membership (among assigned groups only).

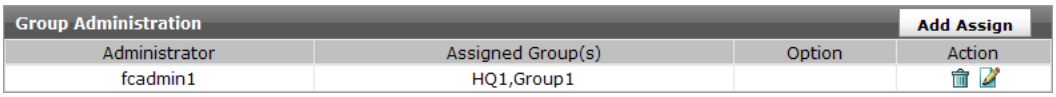
Any FortiManager administrator who does not have the Super_User administrator profile can become a FortiClient Manager group administrator. The permissions settings of the profile apply, except that FortiClient group administrators

- cannot modify FortiClient Manager global settings
- cannot create or edit FortiClient groups
- cannot delete a FortiClient computer
- cannot perform the Search/Add Client function or add a temporary client to the managed clients list
- cannot access clients that belong to another administrator's assigned groups
- cannot set the Roaming status of a FortiClient computer.

Assigning group administrators

In the FortiClient Manager, go to *Settings* > *Group Administration* to view the list of FortiClient group administrators. From this list, you can assign additional group administrators.

Figure 216: List of FortiClient group administrators.



Add Assign	Select to assign client groups to administrators not already listed. See "To assign client groups to an administrator".
Administrator	The group administrator.
Assigned groups	The client group(s) this administrator can manage.
Option	Shows "Allow access ungrouped client(s)" if that option is enabled. Otherwise, the field is blank.

Action

Edit icon	Select to modify client group assignments or options for this administrator.
Delete icon	Select to delete the client group assignments for this administrator. This does not delete the administrator or the client groups.

To assign client groups to an administrator

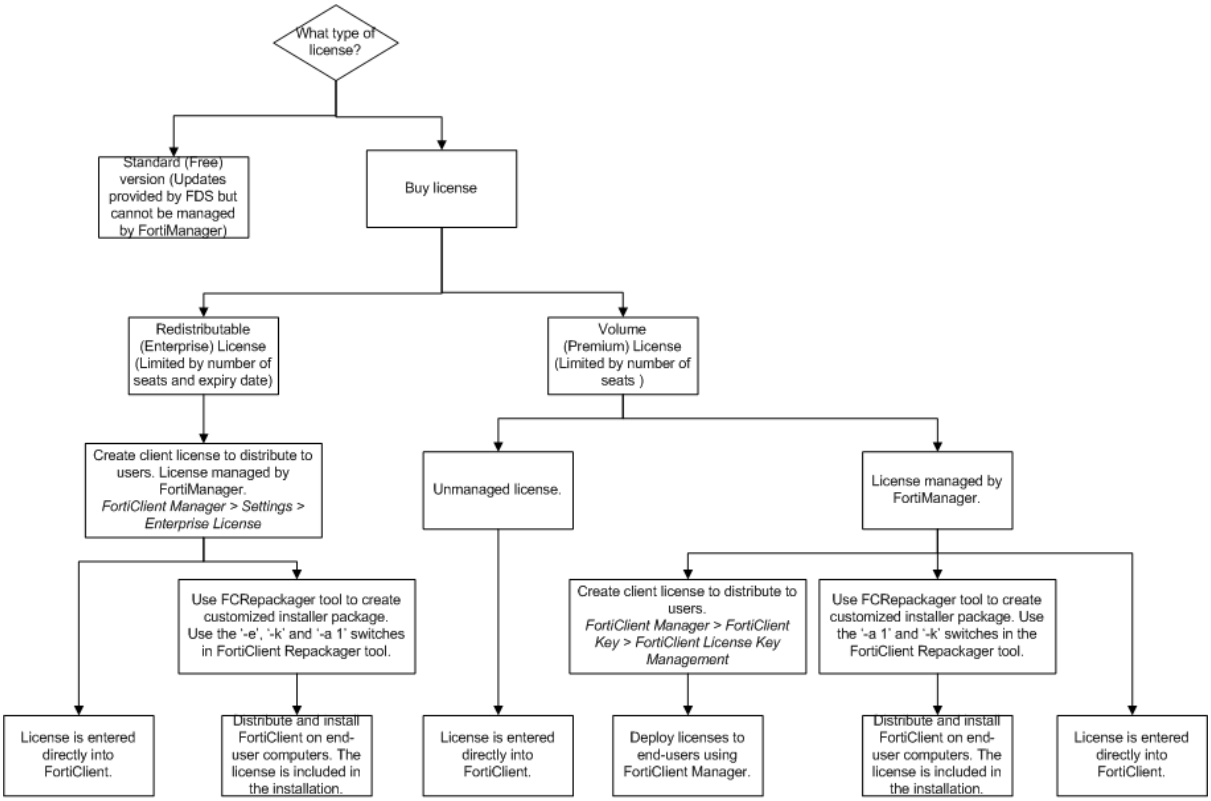
1. In the FortiClient Manager, go to *Settings* > *Group Administration* and select *Add Assign*.

   The *Edit Assigned Groups* page opens.
2. From the *Administrator* list, select the administrator.

   Only administrators who do ***not*** have the Super_User profile are available. The administrator must have read-write access to the FortiClient Manager configuration to modify FortiClient computer settings.
3. Optionally, select *Allow access ungrouped client(s)*.
4. In the *Available Groups* list, select the client groups that this administrator will manage and select the right-pointing arrow to move them to the *Selected Groups* list.
5. Select *OK*.

Configuring enterprise license management

Figure 217: FortiClient licensing.



With Enterprise (Redistributable) licensing, you obtain a re-distributable license from FortiCare and subdivide that license into smaller “seat’ licenses for your users. You can set the expiry date and seat count for each client license. The expiry date of your client licenses cannot be later than that of the enterprise license. The total seat count limit of your client licenses can exceed the seat count limit of the enterprise license, but the total number of managed clients cannot. FortiClient redistributable licensing can be validated by FortiClient Manager or by a company’s own licensing validation system. For more information on internal validation, see the *FortiClient Administration Guide*.

The Redistributable license key can also be given to users and input into FortiClient manually.

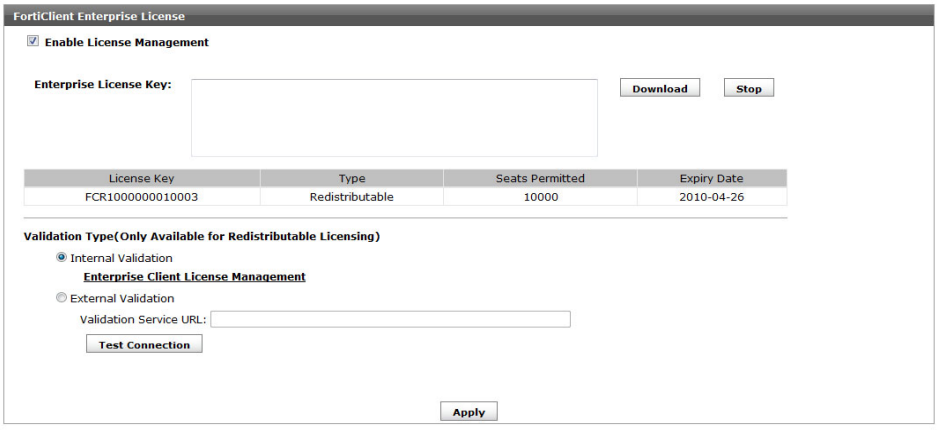
To use enterprise licensing, you need to:

- Obtain an Enterprise License from FortiCare and register it on your FortiManager unit.
- Create at least one enterprise client license for your FortiClient computer. See “Configuring an enterprise license” on page 341.
- Create a custom FortiClient installer that enables enterprise licensing. You can include the client license key in the installer or provide the client license key to users to apply after installation. The FortiClient application must be specifically customized for use with re-distributable licensing. You can use the FCRepackager tool to create a customized installer package that includes the redistributable license. Use the “-a”, “-e” and “-k” switches. For more information, see the *FortiClient Administration Guide* and the *FCRepackager Read-Me* file.
- Deploy the customized FortiClient installer to your users.

Configuring an enterprise license

In the FortiClient Manager, go to *Settings* > *Enterprise License* to configure enterprise licensing. Enter the following information and select *Apply*.

Figure 218: FortiClient Enterprise License configuration.



Enable License Management	Select the check box to use the FortiManager unit to manage licensing of FortiClient computers.
Enterprise License Key	Enter the license key purchased from FortiCare. Select *Download* to register the license. Information about the license appears below this field.
Validation Type	This section is available only if you downloaded a redistributable license.

Internal Validation	Use the FortiManager unit to validate FortiClient license keys.
Enterprise Client License Management	Select this link to create enterprise client license keys for your FortiClient computers. For more information, see "Creating an enterprise client license key" on page 342.
External Validation	Use an external license key validation service.
Test Connection	If you are using external validation, select this button to confirm that the FortiManager unit can communicate with the external validation service.

Creating an enterprise client license key

After you register your enterprise license (see "Configuring an enterprise license" on page 341), you can create enterprise client licenses. For each of these licenses, you can set the expiry date and the seat limit. Client license expiry dates and the total number of seats licensed through enterprise client licenses cannot exceed the limits of the enterprise license.

To create enterprise client license keys

1 Go to *Settings* > *Enterprise License* to configure the enterprise license.

For more information, see "Configuring an enterprise license" on page 341.

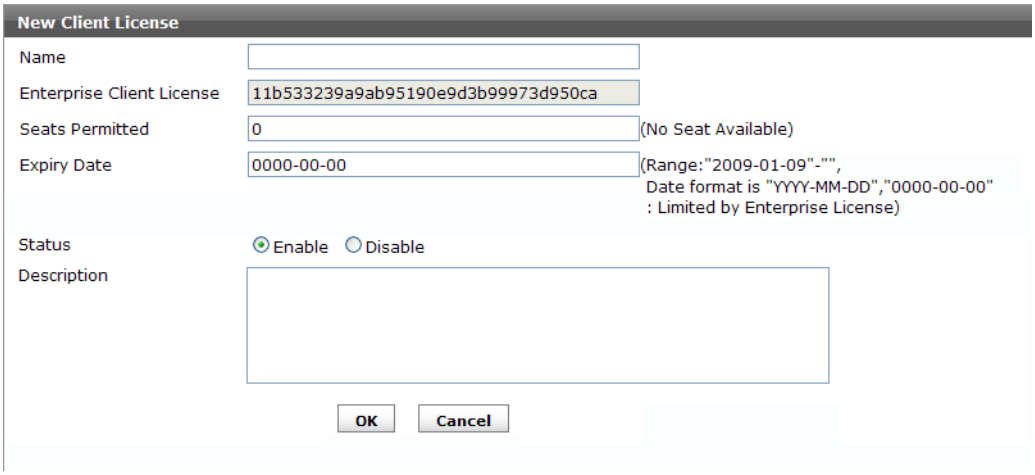
2 Select the *Enterprise Client License Management* link.

The list of enterprise client licenses is displayed.

3 Select *Add*.

The *New Client License* dialog opens, with an enterprise client license key value in place.

Figure 219: New enterprise client license.



4 In the *Name* field, enter a name to identify the license.

5 In the *Seats Permitted* field, enter a number seats that is within the range shown at the right.

The maximum number of seats allowed is the enterprise license limit minus the number of enterprise client licenses actually issued to FortiClient computers.

The total seats permitted in all enterprise client licenses can exceed the enterprise client limit. The FortiManager unit enforces the enterprise license limit only on the actual number of managed enterprise-client licensed FortiClient computers.

6 In the *Expiry Date* field, enter a date that is no later than that of the enterprise license.
7 Optionally, enter a description.
8 Select *OK*.

Creating a customized FortiClient installer

An enterprise client license key is effective only on FortiClient installations that are customized to accept an enterprise license instead of a standard fixed license. For more information, see the FortiClient Administration Guide. Distributing the customized FortiClient installer

You can distribute the customized FortiClient installer in various ways:

- Put the installer on a file share. Users simply double-click the file to begin installation.
- On a Windows Advanced Server network, install the application on end users' computers remotely. For more information, see "Installing FortiClient using Active Directory Server" in the Installation chapter of the FortiClient Administration Guide.

Configuring FortiClient computer settings

You can configure managed FortiClient computers individually or in groups. All the configuration changes are stored in the FortiManager database until they are installed on the FortiClient computers.

For information on installing configuration changes on FortiClient computers, see "Deploying FortiClient computer configurations" on page 324.

When a FortiClient computer is a member of a group, most of its configuration is inherited from the group. You can only change an inherited setting by first selecting the Override option for that part of the configuration. You can reapply the group settings by selecting Apply to All Members in the group configuration.

To configure an individual FortiClient computer

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

   You can also select *Client/Group* > *Group*, then select the group to which the client belongs.

2 From the *Host Name* column of the list of clients, select the client you want to edit.

   From the FortiClient menu, select the part of the configuration you want to edit, *Firewall* > *Policy* for example.

3 Reconfigure the client as needed and then select *Apply*.

To configure a group of FortiClient computers

1 In the FortiClient Manager, in the Navigation Pane, select *Client/Group* > *Group*.
2 From the *FortiClient Group* list, select the name of the group that you want to configure.
3 From the FortiClient menu, select the part of the configuration you want to edit, *Firewall* > *Policy* for example.
4 Reconfigure the settings for the group as needed and then select *Apply*.

   For more information about configuring groups of clients, see "Configuring settings for client groups" on page 322.

Viewing system status of a FortiClient computer

You can display the managed FortiClient computers and view a computer's detailed information.

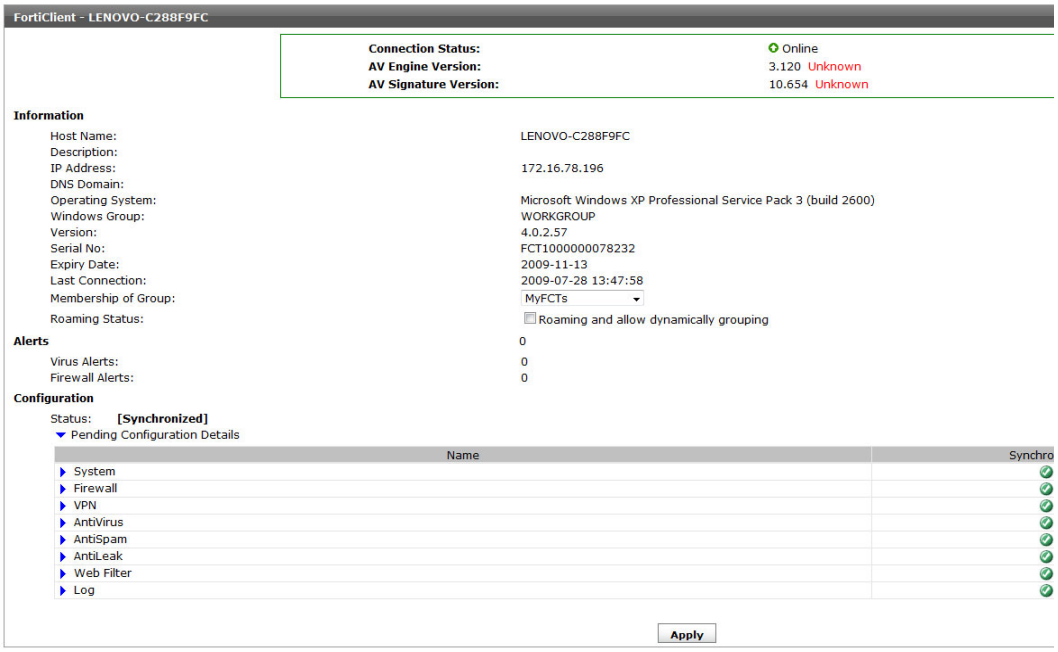
To view detailed FortiClient computer system status information

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want from the *Host Name* column.

3 From the FortiClient menu, select *General* > *Status*.

Figure 220: System status.



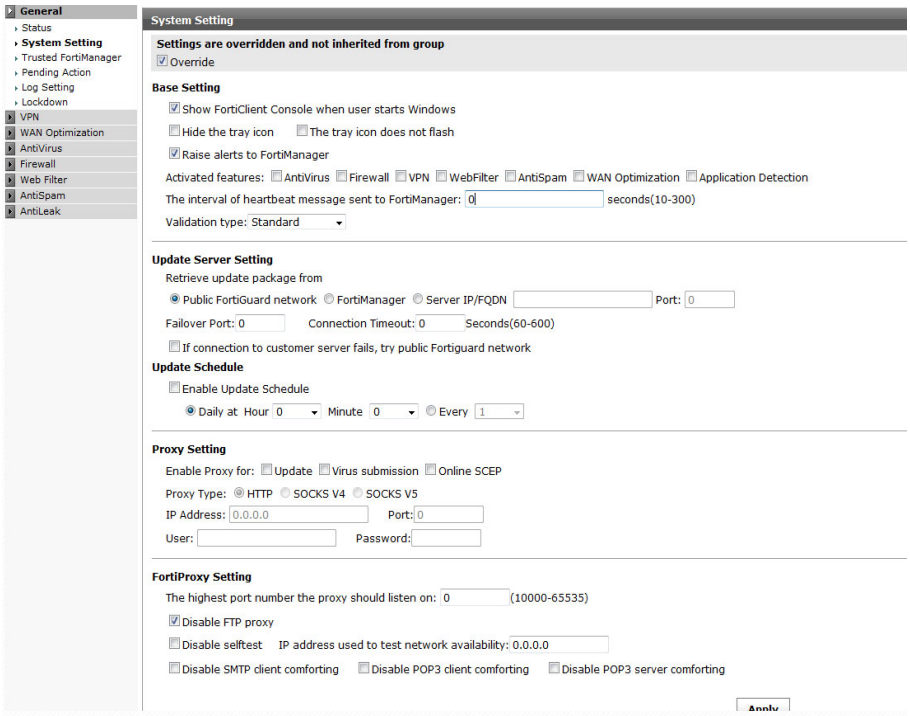
Connection Status	Indicates if the FortiClient computer is connected to the FortiManager unit. Online means connected. Offline means disconnected.
AV Engine Version	Displays the FortiClient computer's antivirus engine version number and whether it is up-to-date.
AV Signature Version	Displays the FortiClient computer's antivirus definition version number and whether it is up-to-date.
Information	
Host Name	The name of the FortiClient computer.
Description	The description from the FortiManager database.
IP Address	The IP address of the FortiClient computer.
DNS Domain	The DNS domain for the computer.
Operating System	The FortiClient computer operating system.
Windows Workgroup	The Windows Workgroup, if applicable.
Version	The FortiClient software version on the computer.

	Serial No	The serial number of the FortiClient computer.
	Expiry Date	FortiClient software license expiry date.
	Last Connection	The time and date when the FortiClient computer last connected to the FortiManager unit.
	Membership of Group	Drop-down list shows the FortiClient group to which the computer belongs or Ungrouped. Optionally, you can select a different group.
	Roaming and allow dynamically grouping	Enable roaming and dynamic grouping for the FortiClient computer. Roaming computers are dynamically grouped when they change IP address. FortiClient Manager sends the new group configuration to the FortiClient computer.
Alerts	Displays the total number of alerts on the FortiClient computer.	
	Virus Alerts	Displays the number of virus alerts on the FortiClient computer.
	Firewall Alerts	Displays the number of firewall alerts on the FortiClient computer.
Configuration		
	Status	Indicates if the configuration changes made on the FortiClient computer through the FortiManager unit have been installed on the FortiClient computer itself. • Synchronized: The changes are installed. • Configuration Pending: The changes are not installed. For information on installing configuration changes, see "Deploying FortiClient computer configurations" on page 324.
	Pending Configuration Details	Displays the configuration changes made on the FortiClient computer through the FortiManager unit that have been installed on the FortiClient computer and those that have not been installed. • A green check mark following a configuration name means the changes are installed. • A gray cross mark following a configuration name means the changes are not yet installed.
Apply		Save the configuration changes.

Configuring system settings of a FortiClient computer

You can configure a FortiClient computer's settings. You can also inherit system settings from the group to which the computer belongs.

Figure 221: System settings.



To configure FortiClient computer system settings

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want from the *Host Name* column.

3 From the FortiClient menu, select *General* > *System Setting*.

Base Setting	
Override	This option is visible only if the FortiClient computer belongs to a group. The FortiClient computer's configuration includes settings inherited from the group. Selecting override allows you to modify the inherited system settings on this FortiClient computer. Deselecting override means that you want to use the system settings inherited from the group to which the computer belongs. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Show FortiClient console when user starts Windows	If selected, the FortiClient program will automatically run when the FortiClient computer starts up.
Hide the tray icon	Select to hide the FortiClient icon in the system tray. It will be active after FortiClient is restarted.
The tray icon does not flash	Select to not have the tray icon flash during antivirus scanning.
Raise alerts to FortiManager	If selected, the FortiClient computer will send alert information to the FortiManager unit.

Activated features	Select the features to be activated in FortiClient. When selected, the features will appear in FortiClient and the feature's services will affect the system. When clear, the features will be removed from FortiClient and the feature's services will be completely inactive. When deactivated, the features should still be configurable from FortiClient Manager although the configuration will not have any affect on the device. If the feature was not installed by the MSI, then it is not possible to activate the feature. To use this effectively, the full FortiClient product needs to be installed. It is possible to repackage the MSI so that although the feature is installed and it is initially 'deactivated'.
The interval of heartbeat message sent to FortiManager	Enter the number of seconds (10-300)
Validation type	Select the license validation type: Standard or Enterprise.
Update Server Setting	
Retrieve update package from	Select the source of FDS updates (AV, Web Filter, Anti-spam): • public FortiGuard network • the FortiManager unit for this computer • another server that you specify
Failover Port	Enter a valid port number.
Connection Timeout	Enter the connection timeout (60-600) in seconds. The default is 60.
If connection to customer server fails, try public FortiGuard network	Select to use the FortiGuard network if your enterprise server fails.
Update Schedule	
Enable Schedule update	Select to enable the update schedule. Enter the Daily time in hour and minutes or the number of hours.
Proxy setting	
Enable proxy for	If internet access from the FortiClient computer is installed on is via a proxy server, FortiClient may need to be configured with the details of that proxy so that it can • Updates - obtain updates • Virus submission - Submit suspicious files for analysis • Online SCEP - Perform certificate operations with remote servers.
Proxy/ Type/ IP Address/ Port	Select the proxy type and enter the IP address and port number for the proxy server.
User, Password	Enter the user name and password for the proxy server.
FortiProxy Setting	
The highest port number the proxy should listen on	Enter the number of ports the server can bind to. It should bind to as many ports as it needs starting at the highest port number specified here. If you have other server service that requires a specific port be left open, you should set the highest port number for FortiProxy to be less than that port number.
Disable FTP proxy	Select to disable the FTP proxy. FortiProxy tests network connectivity by sending packets to a designated IP address.

Disable selftest	Select to disable self test and enter the IP address used to test the network availability.
Disable SMTP client comforting/ Disable POP3 client comforting/ Disable POP3 server comforting	Some email clients may expect response packets from the smtp/pop3 server quickly after the packet was sent. Because FortiProxy may cache the outgoing packets, and incoming server response until all the packets are scanned for malware/spam, the client application may throw a “response timeout” error. When client comforting is enabled, FortiProxy will "drip" packets to the client at a rate that is fast enough to stop the client from erroring, but slow enough to stop the entire response being sent to the client before the response from the server is fully scanned. Select the check boxes to disable these features.

Adding trusted FortiManager units to a FortiClient computer

When installing the FortiClient software, users must set up at least one trusted FortiManager unit. (For more information, see *FortiClient Software v3.0 Release Notes*.) Later, you can add more trusted FortiManager units through the FortiClient Manager and push them to the FortiClient computers. Then the FortiClient computers can be managed by the trusted FortiManager units.

Figure 222: Trusted FortiManager units.

Create New	Select to add a FortiManager unit to manage FortiClient computers.
Override	The FortiClient computer’s configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited trusted FortiManager configuration on this FortiClient computer. Deselecting override means that you want to use the trusted FortiManager configuration inherited from the group to which the computer belongs. Even with inherited trusted FortiManager configurations, you can still add new trusted FortiManager units for a FortiClient computer. See “Adding a FortiClient computer group” on page 320 and “Configuring settings for client groups” on page 322.
Name	Name of a trusted FortiManager unit.
Trusted FortiManager	IP address/range of a trusted FortiManager unit.
Comments	Any notes for a trusted FortiManager unit.
Action	Select the Delete icon to remove a trusted FortiManager unit, and the Edit icon to modify the values of a trusted FortiManager unit. When configuring a group, to copy the trusted FortiManager definition to other groups select Copy to other group.

To add a trusted FortiManager unit

1. In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.
2. In the *All Managed Clients* list, select the FortiClient computer you want from the *Host Name* column.

3 From the FortiClient menu, select *General* > *Trusted FortiManager*.

4 Select *Create New*.

5 In the *Name* field, enter a unique name for the trusted FortiManager unit.

6 From the *Type* list, select the type of address information you have for the trusted FortiManager unit and enter it in the field.

- **Single Address** — the IP address of the unit.
- **IP Range** — the IP range that includes the unit.
- **Subnet** — the IP address and netmask of the subnet that includes the unit.
- **FQDN** — the fully qualified domain name of the unit.

7 Optionally, add information about the unit in the *Comments* field.

8 Select *OK*.

Managing pending actions for a FortiClient computer

The Pending Action page displays the action items to be executed on the selected FortiClient computer by the FortiManager unit. The queue appears when the action items cannot be executed instantly due to reasons such as the FortiClient computers are offline or behind firewalls. It disappears when the actions are successfully completed. The action items include:

- Install configuration: install configuration changes to a FortiClient computer. See “Deploying FortiClient computer configurations” on page 324.
- Retrieve configuration: resynchronize with a FortiClient computer by pulling the FortiClient configurations from the computer and save it to the FortiManager database. See “Retrieving a FortiClient computer configuration” on page 324.
- Notify AV engine/database upgrading: a FortiClient computer’s antivirus engine/database expires.
- Change lockdown configuration: enable or disable lockdown on a FortiClient computer. See “Configuring Lockdown Settings” on page 351.

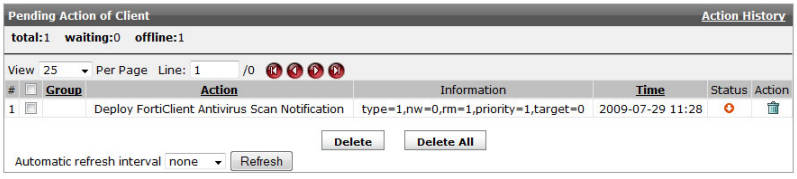
To display the pending actions of a FortiClient computer

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want from the *Host Name* column.

3 From the FortiClient menu, select *General* > *Pending Action*.

Figure 223: Pending actions for a FortiClient computer.



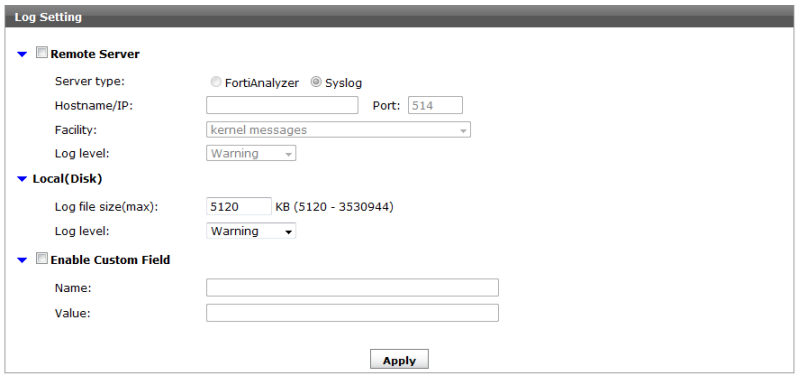
View Per Page	Select the maximum number of actions to display per page.
Page controls	Go to the first, previous, next or last page of the list.
Action	The action items to be executed.

Information	The most up-to-date AV Signature/AV engine version numbers on the FortiManager unit. This information only applies to the Notify AV engine/database upgrading action.
Time	When the action was initiated.
Action	Delete icon - Deletes the action item manually.
Delete	Delete the selected pending actions.
Delete All	Delete all pending actions.

Configuring the log settings of a FortiClient computer

You can configure logging of different types of events for any or all of the FortiClient services by specifying the log level, log type, log size, and log entry lifetime.

Figure 224: Log settings.



To configure log settings

1. In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.
2. In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *General* > *Log Setting*.
4. Configure the following settings and select Apply.

Override	The FortiClient computer's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited remote log settings on this FortiClient computer. Deselecting override means that you want to use the remote log settings inherited from the group to which the computer belongs. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Remote Server	Select to save the logs to a remote FortiAnalyzer or Syslog unit.
Server type	Select *FortiAnalyzer* or *SysLog* as required.
Hostname/IP	Enter the FQDN or IP address of the logging server.
Facility	Select the Facility setting as required. Facility is one of the information fields associated with a log message. If each FortiClient installation is configured to use a different facility setting, you can easily determine the source of a FortiClient log message.
Log level	Select the minimum severity of message to be logged. You can select *Error*, *Warning* or *Information*. The default is *Warning*.
Local (Disk)	These settings apply to logging on the FortiClient computer.

	Log file size (max)	Enter the maximum space allocated to FortiClient logs. The default is 5120 KB. Log entries are overwritten, starting with the oldest, when the maximum log file size is reached.
	Log level	Select the minimum severity of message to be logged. You can select *Error*, *Warning* or *Information*. The default is *Warning*.
Enable Custom Field		Enable the following custom log field to be included in all logs from this FortiClient computer. This field can be used in generating reports on the FortiAnalyzer unit.
	Name	Enter the name of the custom log field.
	Value	Enter the value of the log field.

5 Select *Apply*.

Configuring Lockdown Settings

When Lockdown is enabled, all configuration on the selected FortiClient computer will be read-only at the computer. Users cannot remove the software and cannot change the settings. However, users can connect and disconnect VPN tunnels and can change certificates and CRLs.

If you want to allow the FortiClient user to modify the configuration, you can set the lockdown password and send it to the user who can then use the FortiClient override feature to unlock the configuration.

For global FortiClient Lockdown settings, see "Configuring FortiClient Manager system settings" on page 330.

To configure Lockdown settings

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *General* > *Lockdown*.

4 Select the *Settings are inherited from group* check box to inherit the settings from the group.

5 Select the *Enable Lockdown* check box.

6 Enter the password and click *Apply Lockdown*.

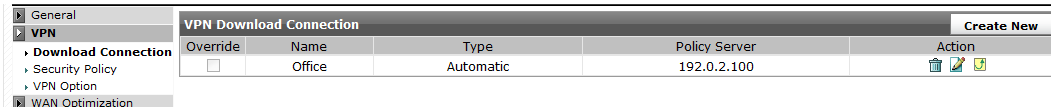
Configuring the VPN settings of a FortiClient computer

The FortiClient Manager can automatically download a VPN setting from the FortiGate unit running FortiOS 3.0 or higher to which your FortiClient computer connects.

If the VPN gateway that your FortiClient computer connects to is a FortiGate unit running FortiOS 2.80 or earlier, or it is a third-party gateway, you must configure the FortiClient VPN settings on the FortiClient computer manually. See the *FortiClient Host Security Version 3.0 User Guide*.

Note: If the computer is locked down by FortiClient Manager, you cannot change the VPN configuration. However, you can connect or disconnect VPN tunnels that are already configured. Lockdown can be applied globally (see "Configuring FortiClient Manager system settings" on page 330) or on specific FortiClient computers (see"Configuring system settings of a FortiClient computer" on page 345).

Figure 225: VPN.



Create New	Select to create a VPN.
Override	The FortiClient computer's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited VPN policy on this FortiClient computer. Deselecting override means that you want to use the VPN policy inherited from the group to which the computer belongs. Even with inherited VPN policies, you can still create new VPN policies for a FortiClient computer. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Name	The name for the VPN.
Type	The type of methods used to create VPNs. In this release, only the automatic method is supported.
Policy Server	The IP address of the VPN gateway, that is, the FortiGate unit running FortiOS 3.0 that the FortiClient computer connects to.
Action	Select the Delete icon to remove a VPN, and Edit icon to modify a VPN. Select Copy to Group to add this configuration to the group to which this FortiClient computer belongs.

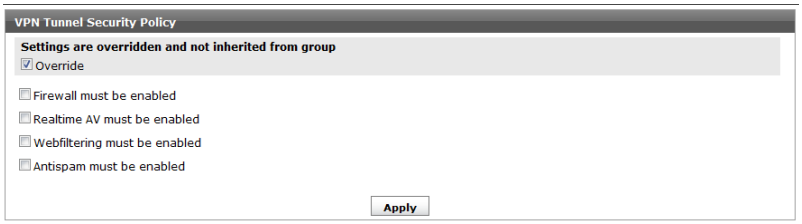
To configure VPN settings

1. In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.
2. In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *VPN* > *Download Connection*.
4. Select *Create New*.
5. Enter a descriptive name for the VPN connection.
6. For *Category*, select *Automatic*.
7. For *Policy Server*, enter the IP address of the VPN gateway.
8. Select *OK*.

Configuring a VPN security policy on a FortiClient computer

For enhanced network security, you can require the FortiClient computer to have security features active before it initiates a VPN connection.

Figure 226: VPN tunnel security policy.



To configure a VPN security policy

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *VPN* > *Security Policy*.

4 Select any of the following policies that you want to enforce:

- Firewall must be enabled
- Realtime AV must be enabled
- Webfiltering must be enabled
- Antispam must be enabled

5 Select *Apply*.

Configuring VPN options of a FortiClient computer

Set the VPN options for computers running FortiClient.

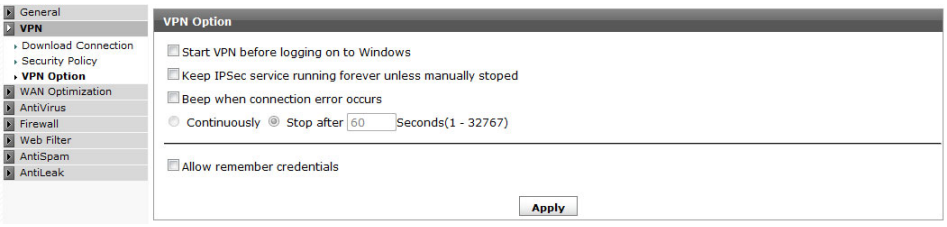
To set the VPN options

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *VPN* > *VPN Option*.

Figure 227: VPN option.



4 Select *Start VPN before logging on to Windows* if you need to log on to a Windows domain through a VPN when you start up your Windows workstation.

5 Select *Keep IPSec service running forever unless manually stopped* to to retry dropped connections indefinitely. By default, the FortiClient software retries a dropped connection four times.

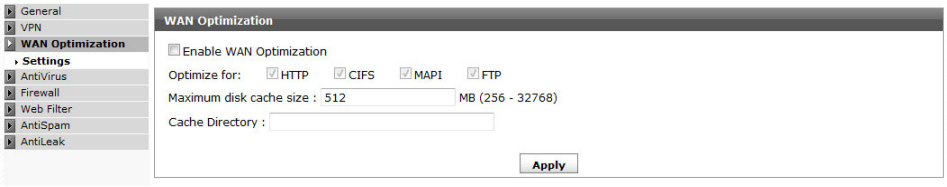
6 Select *Beep when connection error occurs* if you want the FortiClient software to sound a beep when a VPN connection drops. By default, the alarm stops after 60 seconds, even if the connection has not been restored. You can change the duration or select *Continuously* so that the alarm stops only when the connection is restored.

7 Select *Allow remember credentials* to allow eXtended Authentication VPN credentials for a tunnel to be remembered and automatically used the next time the user tries to connect to the VPN tunnel. See the *FortiClient Endpoint Security Guide* for more information on eXtended Authentication.

Configuring WAN Optimization settings of a FortiClient computer

FortiClient WAN Optimization can work together with WAN optimization on a FortiGate unit to accelerate network access. FortiClient will automatically detect if WAN optimization is enabled on the optimizing remote gateway it is connected to and transparently make use of the data reduction and compression features available. Data reduction and compression are bidirectional.

Figure 228: WAN Optimization settings.



Override	The FortiClient computer's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited trusted FortiManager configuration on this FortiClient computer. Deselecting override means that you want to use the trusted FortiManager configuration inherited from the group to which the computer belongs. Even with inherited trusted FortiManager configurations, you can still add new trusted FortiManager units for a FortiClient computer. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Enable WAN Optimization	Enable the WAN Optimization feature. Configure the following options.
Optimize for	Select the protocols to optimize: HTTP, CIFS, MAPI, FTP
Maximum disk cache size	Set maximum disk cache size. Range is 256 to 32 768 MBytes. Entry is rounded to nearest 64MBytes (values 256, 320, 384, and so on). If your hard disk can accommodate a larger cache, better optimization performance is possible.

To enable WAN Optimization

1. In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.
2. In the *All Managed Clients* list, select the FortiClient computer you want from the *Host Name* column.
3. From the FortiClient menu, select *WAN Optimization* > *Settings*.
4. Select *Enable WAN Optimization*.
5. Enable the protocols to be optimized: *HTTP* (web browsing), *CIFS* (file sharing), *MAPI* (Microsoft Exchange) and *FTP* (file transfers).
6. Set *Maximum Disk Cache* to 512, 1024, or 2048MB.

   The default is 256MB. If your hard disk can accommodate a larger cache, better optimization performance is possible.
7. Select *Apply*.

Configuring antivirus settings on a FortiClient computer

The antivirus feature allows you to protect your computer by regularly scanning the computer for viruses. You can also configure real-time virus protection.

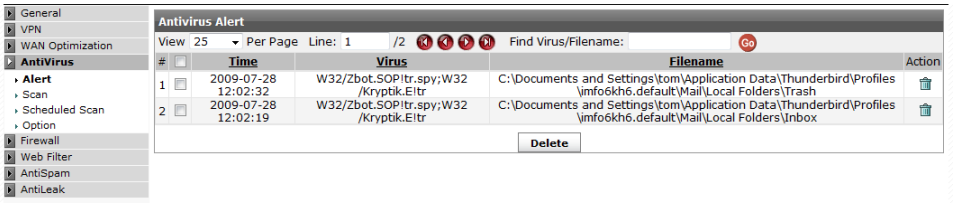
To view antivirus alerts

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *AntiVirus* > *Alert* to view the viruses found on the selected computer.

Figure 229: Antivirus alerts.



Find Virus/Filename	Enter the name of a virus and select Go to search for it.
Delete All	Select to delete all virus alerts.
#	The virus identifier. Viruses are numbered in the order they are found.
Time	The time when the virus was found.
Virus	The name of the virus.
Filename	The virus-infected files

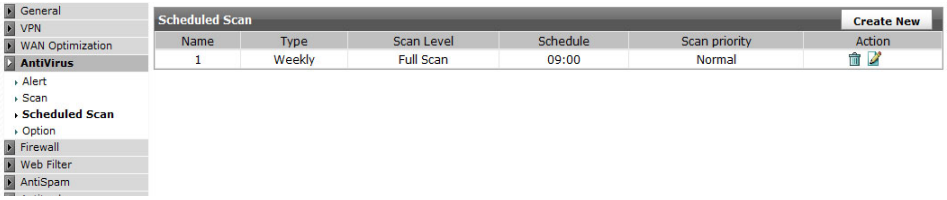
To view virus scan schedules

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *AntiVirus* > *Scheduled Scan*.

Figure 230: Antivirus scheduled scan.



Create New	Select to create a virus scan schedule.
Override	The FortiClient computer's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited virus scan schedule on this FortiClient computer. Deselecting override means that you want to use the virus scan schedule inherited from the group to which the computer belongs. Even with inherited virus scan schedules, you can still create new schedules for a FortiClient computer. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.

Name	Name of the virus scan schedule.
Type	Type of the virus scan schedule: daily, weekly, or one-time.
Scan Level	Indicates whether it is a basic scan or full scan.
Schedule	Timing of the scan. This value is set depending on the type of the virus scan schedule.
Action	Select the Delete icon to remove a virus scan schedule, and Edit icon to modify a virus scan schedule.

To schedule a virus scan

1. In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.
2. In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *AntiVirus* > *Scheduled Scan*.
4. Select *Create New*.
5. Configure the following settings and then select *OK*.

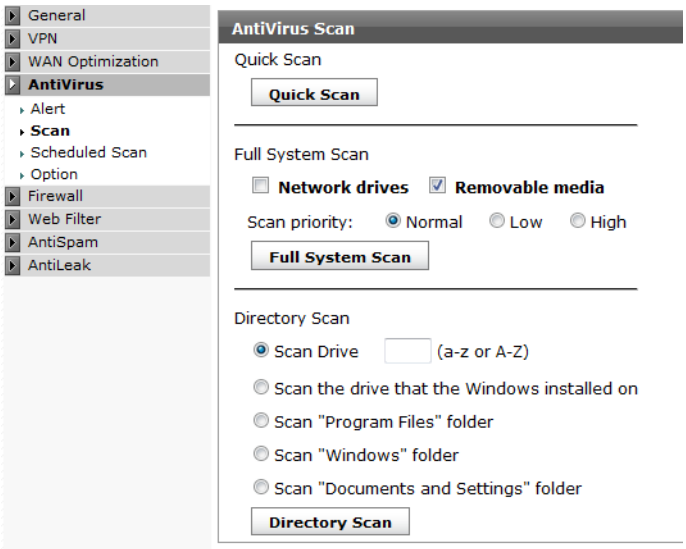
Name	Enter a name for the scheduled scan.
Scan Level	Select a scan level: basic or full scan.
Type	Select the scan frequency. The fields change depending on the type you select. Enter the time, date, and year for the scan accordingly.
Scan Time	Select the scan starting time.

Antivirus scans

The antivirus scan feature enables FortiClient Manager to request FortiClient to perform scans immediately on the target drives and directories specified.

If FortiClient alerts FortiClient Manager if any viruses or malware is found. Virus alerts are visible in the *Message Center* > *Client Alert*.

Figure 231: Antivirus scan.



To do a quick scan

A quick scan scans “in memory” processes and malware using the malware detection engine.

1. In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.
2. In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *AntiVirus* > *Scan*.
4. Click *Quick Scan*.

   The Antivirus Alert page is shown with the list of infected files. See “Viewing antivirus alerts for FortiClient computers” on page 311.

To do a full system scan

1. In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.
2. In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *AntiVirus* > *Scan*.
4. Select *Network drives* or *Removable media* if you want them included in the scan.
5. Select the relative priority of virus scanning compared to other processes
6. Click *Quick Scan*.

   The Antivirus Alert page is shown with the list of infected files. See “Viewing antivirus alerts for FortiClient computers” on page 311.

To do a directory scan

1. In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.
2. In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *AntiVirus* > *Scan*.
4. Select one of the following:
   - Scan drive — Enter the drive letter to scan.
   - Scan the drive that the Windows is installed on
   - Scan “Program Files” folder
   - Scan “Windows” folder
   - Scan “Documents and Settings” folder
5. Click *Directory Scan*.

Configuring antivirus options

You can configure the following antivirus options:

- Email scan options
- Real-time protection options
- Scheduled scan options

- Server protection options
- Quarantine options

Email scan options

You can scan incoming and outgoing email messages and email attachments for viruses and worms.

To configure an email scan

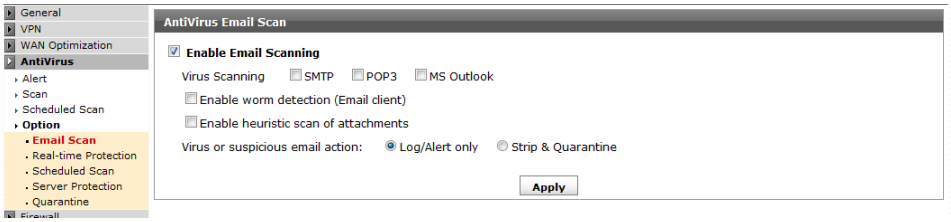
1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *AntiVirus* > *Option* > *Email Scan*.

4 Configure the following settings.

Figure 232: Email scan.



Override	The FortiClient computer's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited email scan configuration on this FortiClient computer. Deselecting override means that you want to use the email scan configuration inherited from the group to which the computer belongs. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Enable e-mail scanning	Select to activate email scanning.
Enable worm detection (Email client)	Select to prevent worms from spreading with emails.
Enable heuristic scan of attachments	Select to scan email attachments to find the unknown viruses and threats that have not yet been cataloged with signatures.
Virus or suspicious email action	**Log/Alert Only** — display a message if a virus is detected during real-time file system monitoring. **Strip & Quarantine** — move the file to a quarantine directory.

Real-time protection options

Configure the real-time protection settings to specify what types of files to scan and exclude and what happens when a virus is detected during real-time system monitoring.

To configure real-time protection

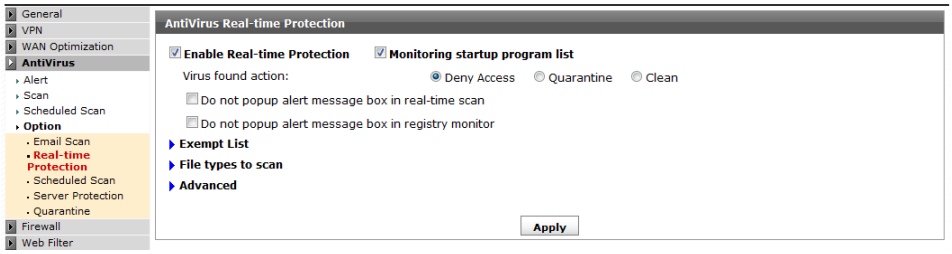
1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *AntiVirus* > *Option* > *Real-time Protection*.

4 Configure the following settings.

Figure 233: Real-time protection.



Override	The FortiClient computer's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited realtime protection configuration on this FortiClient computer. Deselecting override means that you want to use the realtime protection configuration inherited from the group to which the computer belongs. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Enable Real-time Protection	Select to activate real-time protection.
Monitoring startup program list	Select to enable FortiClient to monitor changes to the list of programs that are started automatically when the computer starts.
Virus found action	Select the action FortiClient takes when a virus is found: **Deny Access** — Do not allow user to open, run or modify the file until it is cleaned. **Quarantine** — Move the file to a quarantine directory. **Clean** — Attempt to remove the virus from the infected file. If this is not possible, quarantine the file.
File type exempt list	Use Add to enter the file types that you do not want to scan. Use Delete to remove file types.
File exempt list	Use Add to enter specific files that you do not want to scan. Use Delete to remove files from the list.
Folder exempt list	Use Add to enter the folders that you do not want to scan. Use Delete to remove folders.
Advanced	Optionally, you can: • specify whether to scan compressed files and the file size limit. The default size limit is 0, which means no limit. • specify whether to scan several types of grayware. • enable heuristic scanning. FortiClient software uses heuristic techniques to scan files to find the unknown viruses and threats that have not yet been cataloged with signatures. Heuristics looks at characteristics of a file, such as size or architecture, as well as behaviors of its code to determine the likelihood of an infection. • enable scanning when reading or writing to disk. • enable scanning of network drives.

5 Select *Apply*.

Scheduled scan options

You can set the options for when FortiClient performs a scheduled scan.

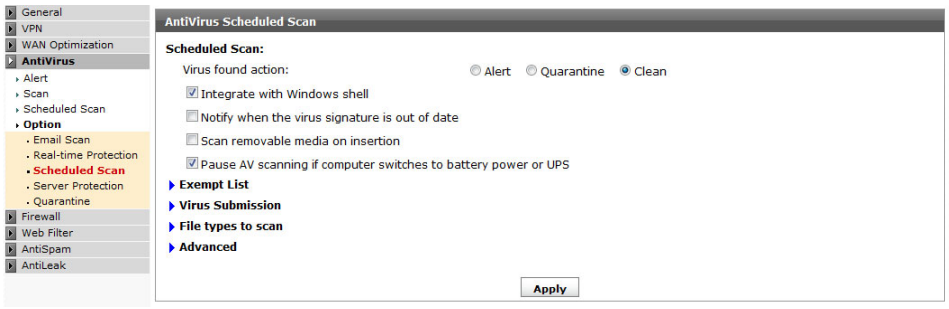
To set scheduled scan options

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *AntiVirus* > *Option* > *Scheduled Scan*.

Figure 234: Antivirus scheduled scan.



4 Configure the following options and then select *Apply*.

Scheduled Scan	
Virus found action	Select one of the following: **Alert** - display a message **Quarantine** - move the file to quarantine **Clean** - attempt to remove the virus from the infected file. If this is not possible, move the file to quarantine.
Integrate with Windows shell	Add a FortiClient antivirus scan command to the Windows Explorer shortcut menu.
Notify when the virus signature is out of date	Although the FortiClient application can alert the user that the virus signature is outdated, if you manage AV updates centrally this notification might confuse users.
Scan removable media on insertion	Enable the FortiClient application to scan removable media, such as USB drives, automatically.
Pause AV scanning if computer switches to battery power or UPS	Enable to reduce drain on batteries by not scanning when the computer is on battery power.
Exempt List	
File type exempt list	This list specifies file types to not scan. To add a file type to the list, enter the file extension in the box and select Add. To remove a file type, select it in the list and then select Delete.
File exempt list	This is a list of specific files to not scan. To add a file to the list, enter the file path in the box and select Add. To remove a file, select it in the list and then select Delete.
Folder exempt list	This is a list of specific folders to not scan. To add a folder to the list, enter its path in the box and select Add. To remove a folder, select it in the list and then select Delete.
Virus Submission	

Use this email account to submit the virus	Instead of using the default mail server, you can specify an SMTP server to use when submitting the quarantined files.
SMTP server	Enter the SMTP server that is used for outgoing mail.
User authentication	If the SMTP server needs authentication to log on, select this check box.
User name	Enter the user name for the SMTP server.
Password	Enter the password for the SMTP server.
Enable automatically submitting suspicious files to Fortinet Inc.	Select to send any suspicious virus files to Fortinet.
File types to scan	
All files	Select to scan all files.
Program files and documents	If you do not want the FortiClient software to scan all files for viruses, select this option.
File types to scan	Enter the file types to scan for.
Files with no extension	Select to scan files that have no extension.
Advanced	
Scan Compressed Files	Scan compressed files, such as .zip files. Enter the maximum size of file to scan. The default size limit is 0, which means no limit.
Scan Grayware	Select the types of grayware that FortiClient looks for while scanning.
Enable Heuristic scanning	FortiClient software uses heuristic techniques to scan files to find unknown viruses and threats that have not yet been cataloged with signatures. Heuristics looks at characteristics of a file, such as size or architecture, as well as behaviors of its code to determine the likelihood of an infection.
AV signature	
Use small DB (Small DB is only supported by FortiClient 4.0)	If you only want to scan for active viruses, select the check box. The core signature database is comprised of viruses that are currently active. This option will take lesser time to scan your computer because of the smaller database. The core signature database does not require a license and is updated frequently.
Use Extended DB (Extended DB is supported by FortiClient 4.1 upwards)	Select the check box if you want to do antivirus scans using the full antivirus database. The extended signature database is comprised of the full antivirus database. Using this option will take a longer time to scan your computer. The extended signature database requires a premium license and is updated less frequently.

Server protection options

You can set the Microsoft Exchange and Microsoft SQL server settings options.

Caution: If Microsoft Exchange or SQL servers are installed, allowing antivirus to scan the product files can cause these products performance problems or cause product failure.

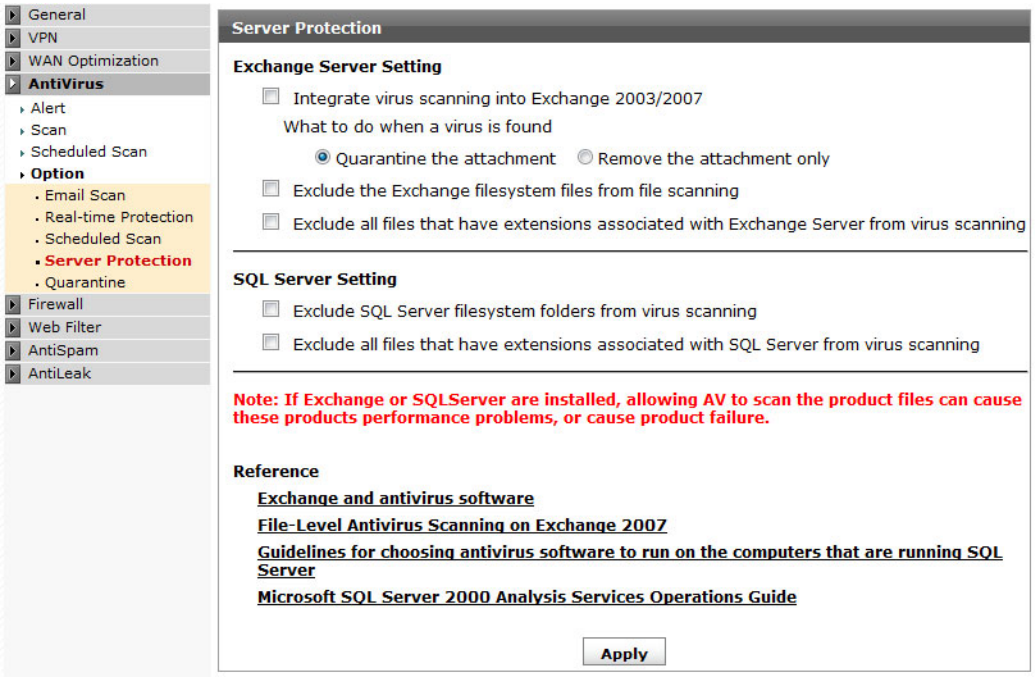
To set the server protection options

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *AntiVirus* > *Option* > *Server Protection*.

Figure 235: Server protection.



4 Configure the following options and then select *Apply*.

Exchange Server Setting	
Integrate virus scanning into Exchange 2003/2007	Select to scan Microsoft Exchange data stores for viruses.
What to do when a virus is found	• Quarantine the attachment — The message and attachment is quarantined. • Remove the attachment only — The infected attachment is removed, but the body of the message remains.
Exclude the Exchange filesystem files from scanning	Fortinet recommends that you enable this setting to avoid impairing the operation of the Exchange server.
SQL Server Setting	
Exclude SQL Server filesystem folders from virus scanning	Fortinet recommends that you enable this setting to avoid impairing the operation of SQL server.
Exclude all files that have extensions associated with SQL Server from virus scanning	Fortinet recommends that you enable this setting to avoid impairing the operation of SQL server.

Quarantine options

You are able to specify the number of days to retain the quarantined files. Quarantine retains all files until you delete or restore them, unless you configure automatic deletion.

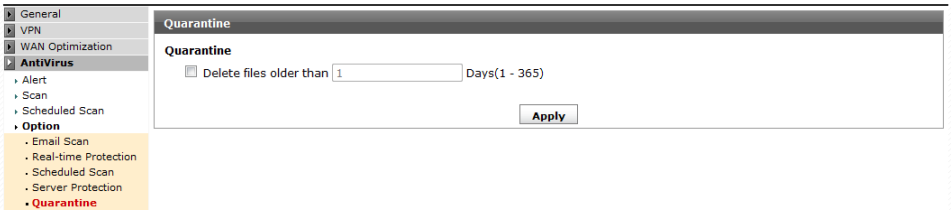
To set the quarantine options

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *AntiVirus* > *Option* > *Quarantine*.

Figure 236: Quarantine.



4 Select the *Delete files older than* check box and enter the number of days to retain files.

5 Click *Apply*.

Viewing the firewall monitor of a FortiClient computer

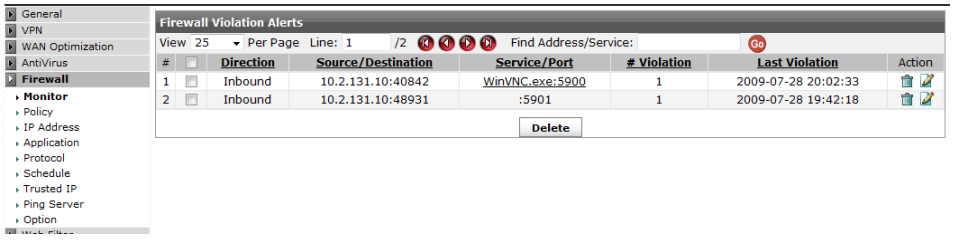
On the FortiClient computer, when an application tries to connect through the firewall, FortiClient Host Security normally prompts the user to allow or disallow the access unless there is a matching firewall policy. When controlled by FortiManager, the FortiClient application blocks all access for which there is no firewall policy and raises a firewall policy violation alert to the FortiManager unit.

Optionally, you can change the FortiClient default to allow all accesses for which there is no Deny firewall policy. See “Setting the firewall options of a FortiClient computer” on page 374.

Based on the violations recorded in the firewall monitor, you can add new firewall policies to allow or disallow these access attempts in future.

Select a FortiClient computer in the All Managed Clients or Ungrouped Clients lists and open its Firewall Monitor. Firewall Monitor displays firewall policy violation events that occur on the managed FortiClient computers.

Figure 237: Firewall monitor.



Source / Destination	The source and destination address to which the policy applies. See "Configuring firewall addresses on a FortiClient computer" on page 366.
Service / Port	Protocols of the connection attempts.
# Violations	The number of firewall policy violations.
Last Violation	The date and time of the most recent violation.
Action	
Delete icon	Select to delete a firewall violation record.
Edit icon	Select to create a policy for a firewall violation event if there is no existing policy for the event. See "To create a policy for a firewall violation event" on page 364.
Delete	Delete the selected firewall violation records for this device.

To create a policy for a firewall violation event

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *Firewall* > *Monitor*.

4 For the firewall violation event that you want to add a policy, select the *Edit* icon.

Destination	Create a new address name or select an existing one. If you create a new address name, this name is linked with this violation event. If you choose an existing address, it may not be linked to this violation event. See "Configuring firewall addresses on a FortiClient computer" on page 366.
Service	Create a new service or select an existing one. If you create a new service name, this name is linked with this violation event. If you choose an existing service, it may not be linked to this violation event. See "Defining firewall protocols on a FortiClient computer" on page 369.
Schedule	Select the schedule that controls when the policy should be active. See "Configuring firewall schedules on a FortiClient computer" on page 371.
Action	Select the response to make when the policy matches a connection attempt.
Comment	Optionally, add any comments you have for this policy.

5 Select *OK*.

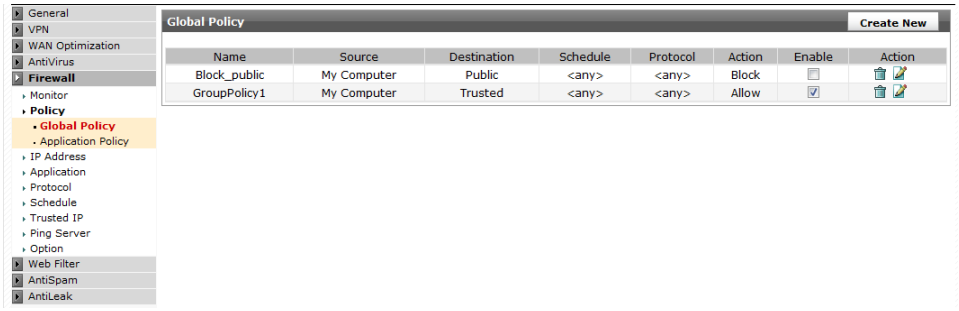
Creating firewall policies on a FortiClient computer

Firewall policies are instructions that the FortiClient program uses to decide what to do with a connection request. When managed by a FortiManager unit, the FortiClient firewall operates in Custom Profile mode.

Create global firewall policies to control traffic generally. These policies create FortiClient advanced firewall rules.

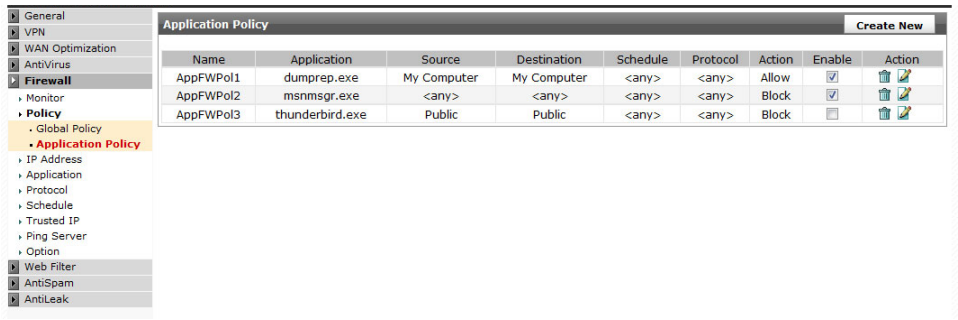
Create application firewall policies to control specific applications' access to the network. These policies create FortiClient advanced application firewall rules.

Figure 238:



Global firewall policy.

Figure 239: Application Firewall policy.



Create New	Create a firewall policy.
Override	The FortiClient computer's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited firewall policy on this FortiClient computer. Deselecting override means that you want to use the firewall policy inherited from the group to which the computer belongs. Even with inherited firewall policies, you can still create new firewall policies for a FortiClient computer. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Name	The policy name.
Application	For an application policy, select the application. If the application is not listed, go to *Application* > *Application* in the FortiClient menu. See "Defining firewall applications on a FortiClient computer" on page 368.
Source	The source address to which the policy applies. See "Configuring firewall addresses on a FortiClient computer" on page 366.
Destination	The destination address to which the policy applies. See "Configuring firewall addresses on a FortiClient computer" on page 366.
Schedule	The schedule that controls when the policy should be active. See "Configuring firewall schedules on a FortiClient computer" on page 371.
Protocol	The service to which the policy applies. See "Defining firewall protocols on a FortiClient computer" on page 369.
Action	The response to make when the policy matches a connection attempt: *Allow* or *Block*.
Enable	Enable or disable the policy. Enabling the policy makes it available for the firewall to match it to incoming or outgoing connections.
Action	Select the Delete icon to remove a policy, and Edit icon to modify a policy.

To create a firewall policy

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select one of the following:

- for a general firewall policy, *Firewall* > *Policy* > *Global Policy*
- for an application-specific policy, *Firewall* > *Policy* > *Application Policy*

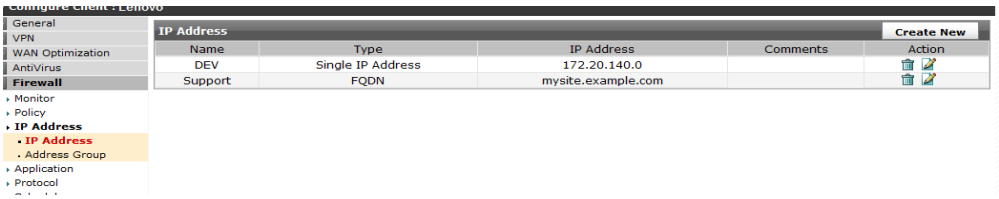
4 Select *Create New*.

5 Enter the field value as described above and then select *OK*.

Configuring firewall addresses on a FortiClient computer

Add, edit, and delete firewall addresses as required. Firewall policies specify firewall addresses to match the source or destination IP addresses of packets that the FortiClient computer receives.

Figure 240: Firewall address.



Create New	Select to create a firewall address for the managed FortiClient computer.
Override	The FortiClient computer's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited firewall address configuration on this FortiClient computer. Deselecting override means that you want to use the firewall address configuration inherited from the group to which the computer belongs. Even with inherited firewall address configurations, you can still create new firewall addresses for a FortiClient computer. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Name	The name of the firewall address.
Type	Select one of *Single Address*, *IP Range*, *Subnet*, or *FQDN*.
Single Address **IP Range** **Subnet** **FQDN**	This name and format of this field depends on the *Type* setting. ***Examples***: • Single Address: `10.10.1.2` • IP Range: `10.10.1.[12-20]` or `10.10.1.12-10.10.1.20` • Subnet: `10.10.10.0/255.255.0.0` • FQDN: `mysite.example.com`
Comments	Comments on the firewall address.
Action	**Delete** — Remove the selected firewall address. **Edit** — Modify the firewall address. **Copy to group** — If the FortiClient computer belongs to a client group, add this address to the group configuration.

To add a firewall address

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want from the *Host Name* column.

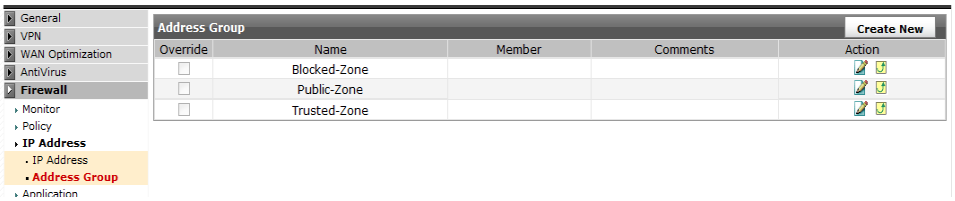
3 From the FortiClient menu, select *Firewall* > *IP Address* > *IP Address*.

4 Select *Create New*, enter the information as described above and then select *OK*.

Configuring firewall address groups on a FortiClient computer

You can create groups of firewall addresses for use in firewall policies. The default Address Groups are Blocked-Zone, Public-Zone, and Trusted-Zone. You can edit these Address Groups or create new groups.

Figure 241: Firewall address group.



Create New	Select to create a firewall address group.
Override	The FortiClient computer's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited firewall address group configuration on this FortiClient computer. Deselecting override means that you want to use the firewall address group configuration inherited from the group to which the computer belongs. Even with inherited firewall address group configurations, you can still create new firewall address groups for a FortiClient computer. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Name	The name of the firewall address group.
Member	The addresses in the address group.
Comments	Comments on the firewall address group.
Action	Select the Delete icon to remove a firewall address group, and Edit icon to modify a firewall address group.

To add a firewall address group

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want from the *Host Name* column.

3 From the FortiClient menu, select *Firewall* > *IP Address* > *Address Group* > *Create New*.

Group Name	Enter a name to identify the address group. You must not use the same name as any firewall address or virtual IP.

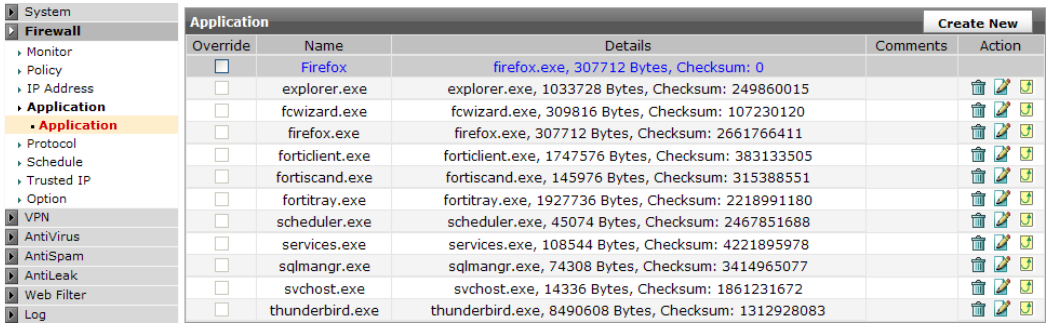
Comments	Optionally, add comments on the firewall address group.
Group Members	Use the arrows to move addresses between the *Available Address* (configured and default firewall addresses) and *Selected Address* lists. The list of addresses come from the IP Addresses.

4 Select *OK*.

Defining firewall applications on a FortiClient computer

Define applications so that you can create firewall policies to allow or deny network access to these applications. For information about creating firewall policies for applications, see “Creating firewall policies on a FortiClient computer” on page 364.

Figure 242: Firewall applications.



Create New	Select to create a firewall application.
Override	The FortiClient computer’s configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited firewall application configuration on this FortiClient computer. Deselecting override means that you want to use the firewall application configuration inherited from the group to which the computer belongs. Even with inherited firewall application configurations, you can still create new firewall applications for a FortiClient computer. See “Adding a FortiClient computer group” on page 320 and “Configuring settings for client groups” on page 322.
Name	The name of the firewall application.
Details	The information about the firewall application, including its executable file name, size, and checksum.
Comments	Comments on the firewall application.
Action	Select the *Delete* icon to remove a firewall application, and *Edit* icon to modify a firewall application.

To define a firewall application

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *Firewall* > *Application* > *Create New*.

Name	Enter a name to identify the application.
Executable File	Enter the executable file name of application. For example, the executable of Internet Explorer is iexplorer.exe. Optionally you can leave this field blank to define the service only by its ports.
File size	Enter the size of the executable file. If *Executable File* is blank, enter a value that is not the same as that of any other application executable file.
Checksum (CRC32)	Enter the CRC32 checksum of the executable file. If *Executable File* is blank, enter a value that is not the same as that of any other application executable file. The checksum and file size are used to uniquely identify the application executable file.
Comments	Enter any comments on the firewall application.

4 Select *OK*.

Defining firewall protocols on a FortiClient computer

Define protocols so that you can create firewall policies to allow or deny use of these protocols. You define a protocol in terms of the UDP or TCP ports that it uses. See "To define a firewall protocol" on page 370.

To make it easier to add policies, create groups of protocols and then add one policy to allow or block access for all the protocols in the group. A protocol group cannot be added to another protocol group. See "Configuring firewall protocol groups on a FortiClient computer" on page 370.

Figure 243: Firewall protocol.

Create New	Select to create a firewall protocol.
Override	The FortiClient computer's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited firewall service configuration on this FortiClient computer. Deselecting override means that you want to use the firewall service configuration inherited from the group to which the computer belongs. Even with inherited firewall service configurations, you can still create new firewall services for a FortiClient computer. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Name	The name of the firewall protocol.
Type	The type of protocol: TCP, UDP, TCP/UDP or ICMP
Source Port	Source port for the protocol.
Destination Port	Destination port for the protocol.
Action	Select the Delete icon to remove a firewall protocol, and Edit icon to modify a firewall protocol.

To define a firewall protocol

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *Firewall* > *Protocol* > *Create New*.

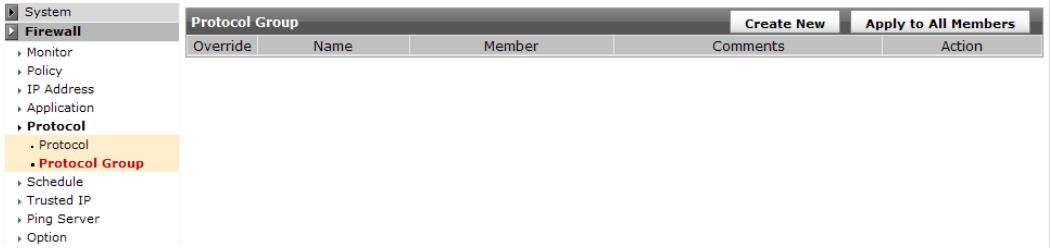
Name	Enter a name to identify the protocol.
Protocol	Select the protocol type: TCP, UDP, TCP/UDP or ICMP.
Source Port	Specify the source port number for the protocol. (Not for ICMP.)
Destination Port	Specify the destination port for the protocol. (Not for ICMP.)
Comments	Enter any comments on the firewall protocol.

4 Select *OK*.

Configuring firewall protocol groups on a FortiClient computer

You can create groups of firewall protocols for use in firewall policies.

Figure 244: Firewall protocol group.



Create New	Select to create a firewall protocol group.
Override	The FortiClient computer's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited firewall protocol group configuration on this FortiClient computer. Deselecting override means that you want to use the firewall protocol group configuration inherited from the group to which the computer belongs. Even with inherited firewall protocol group configurations, you can still create new firewall protocol groups for a FortiClient computer. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Name	The name of the firewall protocol group.
Member	The services added to the protocol group.
Comments	Comments on the firewall protocol group.
Action	Select the Delete icon to remove a firewall protocol group, and Edit icon to modify a firewall protocol group.

To create a firewall protocol group

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *Firewall* > *Protocol* > *Protocol Group* > *Create New*.

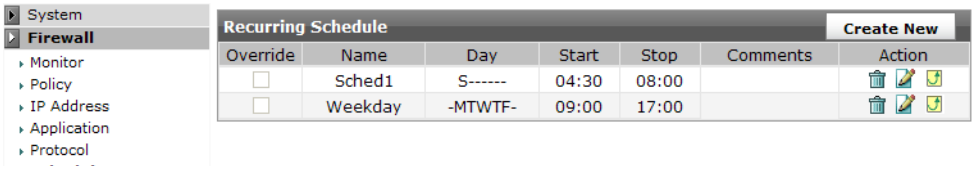
Group Name	Enter a name to identify the protocol group.
Comments	Enter any comments on the firewall protocol group.
Available Protocols	The list of configured protocols. Use the arrows to move protocols between the lists.
Members	The list of protocols in the group. Use the arrows to move protocols between the lists.

4 Select *OK*.

Configuring firewall schedules on a FortiClient computer

Use recurring schedules to control when policies are active or inactive. Recurring schedules repeat weekly and are effective only at specified times of the day or on specified days of the week.

Figure 245: Firewall schedule.



Create New	Select to create a firewall recurring schedule.
Override	The FortiClient computer's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited firewall schedule configuration on this FortiClient computer. Deselecting override means that you want to use the firewall schedule configuration inherited from the group to which the computer belongs. Even with inherited firewall service group configurations, you can still create new firewall schedules for a FortiClient computer. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Name	The name of the firewall schedule.
Day	The start day for the schedule.
Start	The start time for the schedule.
Stop	The stop time for the schedule.
Comments	Comments on the firewall schedule.
Action	Select the Delete icon to remove a firewall schedule, and Edit icon to modify a firewall schedule.

To configure a firewall recurring schedule

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *Firewall* > *Schedule* > *Recurring* > *Create New*.

Name	Enter the name of the firewall schedule.
Comments	Add comments on the firewall schedule, if any.
Day	Select the days of the week when the schedule applies.

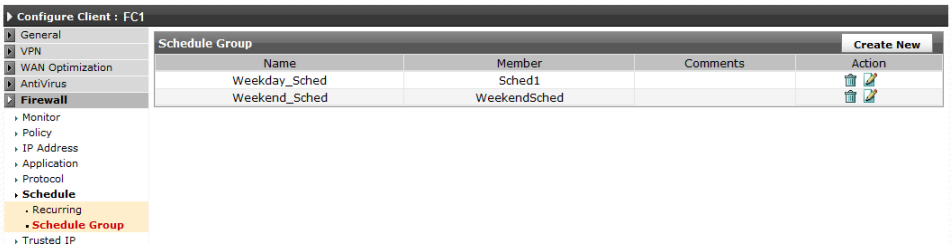
Start	Select the start time for the schedule.
Stop	Select the stop time for the schedule.

4 Select OK.

Configuring firewall schedule groups

You can group the recurring schedules.

Figure 246: Firewall schedule groups.



Create New	Select to create a firewall recurring schedule group.
Name	The name of the firewall schedule group.
Member	Which recurring schedules are members of the group.
Comments	Comments on the schedule group.
Action	Select the Delete icon to remove a firewall schedule, and Edit icon to modify a firewall schedule.

To create a schedule group

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *Firewall* > *Schedule* > *Schedule Group* > *Create New*.

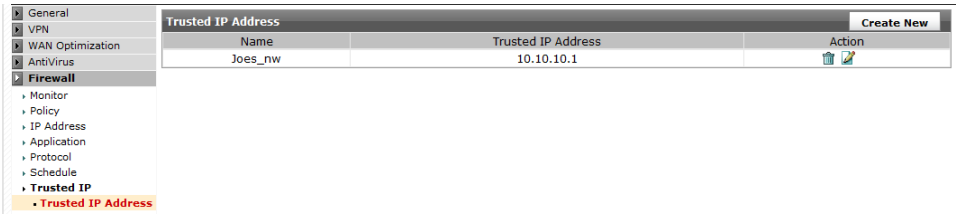
Group Name	Enter the name of the firewall schedule group.
Comments	Add comments on the firewall schedule group, if any.
Available Schedule	List of recurring schedules that are available to be in the schedule group.
Selected Schedule	List of recurring schedules that are members of the group.

4 Select OK.

Configuring trusted IPs exempted from intrusion detection

You can specify trusted IP addresses from which traffic will not be scanned for potential intrusion attempts.

Figure 247: Trusted IP addresses.



To configure trusted IPs

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *Firewall* > *Trusted IP* > *Trusted IP Address*.

4 Select *Create New*.

5 Enter a name for the trusted IP address.

6 Do one of the following:

- From the *Type* list, select *Single Address* and enter the address in the *Single Address* field.
- From the *Type* list, select *IP Range* and enter the IP address range in the *IP Range* field.
- From the *Type* list, select *Subnet* and enter the IP address and subnet mask in the *Subnet* field.

7 Select *OK*.

8 In the FortiClient menu, go to *System* > *Trusted IP* > *Trusted IP Setting* and select the *Enable Trusted IP* check box.

9 Select *Apply*.

Configuring ping servers for a FortiClient computer firewall

You can define ping servers that the FortiClient application checks when it is connected to a new network, such as a wireless access point.

Figure 248: Firewall ping server.

Name	Enter the name for the ping server.
Ping Server	The IP address or fully qualified domain name (FQDN) of the server.
Day	Select the days of the week when the schedule applies.
Action	Select Edit to modify the configuration or Delete to remove it.

To configure a firewall ping server

1. In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.
2. In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Firewall* > *Trusted IP* > *Ping Server*.
4. Select *Create New*.
5. Enter a name for the ping server.
6. Enter the IP address or FQDN of the ping server.
7. Select *OK*.

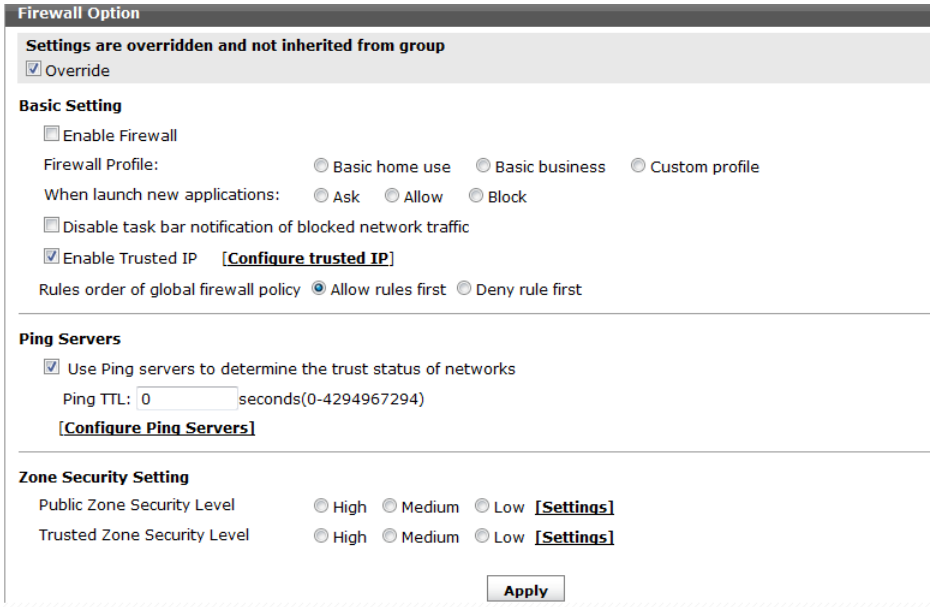
Setting the firewall options of a FortiClient computer

When controlled by FortiManager, the FortiClient application normally blocks all access for which there is no firewall policy and raises a firewall policy violation alert to the FortiManager unit. Optionally, you can change the FortiClient firewall default action to allow all accesses for which there is no Deny firewall policy.

The FortiClient application has three pre-configured firewall profiles: Basic home use, Basic business and Custom. The custom profile is the default. You define firewall policies as needed to allow or deny traffic.

Select a FortiClient computer in the All Managed Clients or Ungrouped Clients lists and select *Firewall* > *Option* to configure the firewall default action.

Figure 249: Firewall Option settings.



Override	Select to override the policy inherited from the group to which the computer belongs.
Basic Setting	
Enable Firewall	Select to enable the firewall.

Firewall Profile	Select one of the following profiles. **Basic home use** — Allow all outgoing traffic and deny all incoming traffic. **Basic business** — Allow all outgoing traffic, allow all incoming traffic from the trusted zone, and deny all incoming traffic from the public zone. **Custom profile** — This is the default profile. You can configure firewall policies to control application access to the network and to control traffic between address groups.
When launch new applications	Select firewall action when an unknown application tries to communicate through the firewall: **Ask** — The user is asked if the application should be allowed or denied network access. This is the default option. **Allow** — Allow the application to communicate, but raise a firewall violation alert. **Block** — The application is blocked and raises a firewall violation alert.
Disable task bar notification of blocked network traffic	Do not alert FortiClient user that traffic is blocked.
Enable Trusted IP	Trusted IP addresses, defined in *Firewall* > *Trusted IP* are not scanned for potential intrusion attempts. See "Configuring trusted IPs exempted from intrusion detection" on page 372.
Rules order of global firewall policy	When there are "allow" and "deny" firewall rules in FortiClient, this setting determines the action that has higher priority when rules overlap. **Allow rules first** — When selected, the "allow" firewall rules in FortiClient are processed first. **Deny rule first** — When selected, the "deny" firewall rules in FortiClient are processed first.
Ping Servers	
Use Ping servers to determine the trust status of networks	The FortiClient application checks for response from ping servers you have configured to determine whether it is connected to a trustworthy network. See "Configuring ping servers for a FortiClient computer firewall" on page 373.
Zone Security Setting	Select the security level for the Public and Trusted zones.
Public Zone Security Level	**High** — Block ICMP, NetBIOS, but allow other traffic coming from this zone. **Medium** — Block ICMP and NetBIOS from this zone, but allow other traffic. Allow NetBIOS to this zone. **Low** — Allow all traffic, except where disallowed by application policies. By default, the Public Zone has High security level.
Trusted Zone Security Level	**High** — Block ICMP, NetBIOS, but allow other traffic coming from this zone. **Medium** — Allow all traffic to and from this zone. **Low** — Allow all traffic, except where disallowed by application policies. By default, the Trusted Zone has Medium security level.

Selecting a web filter profile for a FortiClient computer

If web filtering is enabled, Web filter profiles determine which categories and classifications of URLs are blocked.

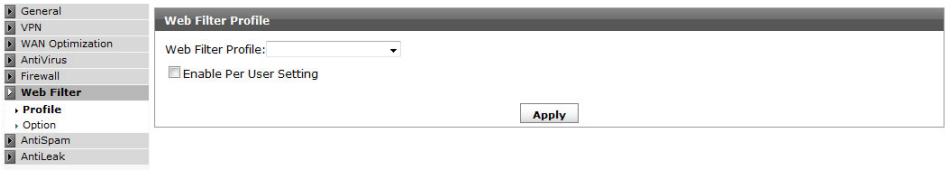
To view web filter profiles

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *Web Filter* > *Profile*.

Figure 250: Web filter profile.



Apply to All Members	If you are editing a group profile, select this button to replace web filter settings on all members with the group settings.
Override	The FortiClient computer's configuration includes settings inherited from the group to which the computer belongs. Selecting override allows you to select a different web filter profile than the one inherited from the group. Deselecting override means that you want to use the web filter profile inherited from the group to which the computer belongs. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Web Filter Profile	Select a web filter profile. For more information, see "Viewing and editing web filter profiles" on page 328. If you select Enable Per User Setting, this profile is applied to users with no assigned web filter profile.
Enable Per User Setting	For a FortiClient computer that belongs to a Windows AD domain, enable this option to select a web filter depending on the computer user based on information retrieved from Windows AD. See "Working with Windows AD users and groups" on page 335.

Configuring web filter options on a FortiClient computer

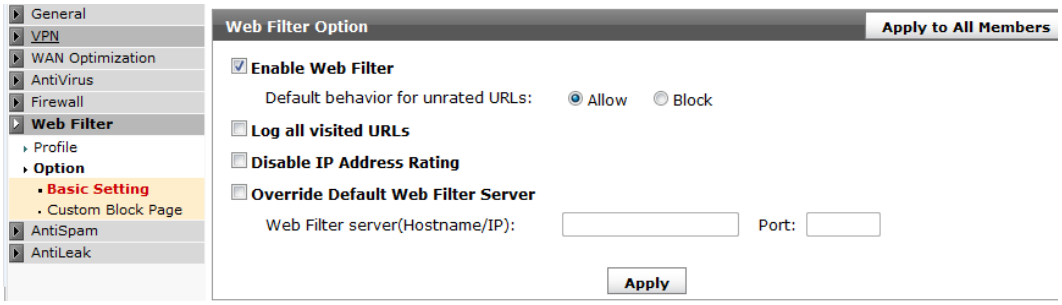
You can enable web filtering that uses the FortiGuard-web filtering service to help you control web access by URL. For FortiClient computers and groups, web filter profiles determine which categories of URLs are blocked and which specific URLs are always blocked or always allowed. See "Viewing and editing web filter profiles" on page 328.

FortiGuard-Web is a managed web filtering solution provided by Fortinet. FortiGuard-Web sorts hundreds of millions of web pages into a wide range of categories users can allow, block, or monitor.

The FortiManager unit can act as the local FortiGuard web filter service center, overriding the default FortiGuard servers. If you have a large number of FortiClient computers, using this feature speeds up the installation of the web filter settings.

You can specify a replacement web page for the FortiClient computer to display to users when a URL is blocked because of its category or because it is in the block site list. See "To configure custom Web Filter Block web pages" on page 377.

Figure 251: Web filter options.



To configure web filter options

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *Web Filter* > *Option* > *Basic Setting*.

4 Configure the following settings and select *Apply*.

Override	The FortiClient computer's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited FortiGuard server on this FortiClient computer. Deselecting override means that you want to use the FortiGuard server inherited from the group to which the computer belongs. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Enable Web Filter	Select to enable web filtering.
Default behavior for unrated URLs	Select whether to allow or block URLs that are not known to FortiGuard Web. The default is *Allow*.
Log all visited URLs	Log all visited URLs to FortiAnalyzer or Syslog server
Disable IP Address Rating	Filter by domain rating only. Sometimes filtering by IP address can produce false positives.
Override Default Web Filter Server	Select to get the web filter settings from the FortiManager unit: • Enter the unit's IP address. • Enter the unit's port number.

To configure custom Web Filter Block web pages

Note: If the Web Filter block page is customized, it MUST be written in UTF-8. Because the URL rating category is in UTF-8, the charset cannot be mixed in one page.

Use the following line to help the web browser select the correct code page to display.

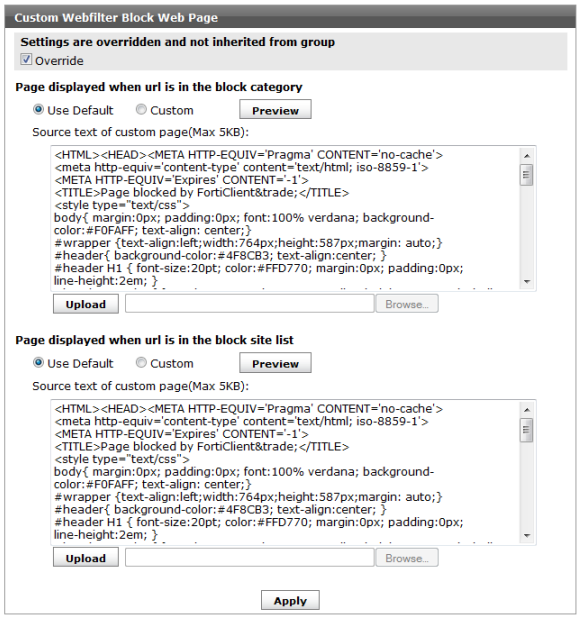
```
<meta http-equiv='content-type' content='text/html; charset=UTF-8'>
```

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *Web Filter* > *Option* > *Custom Block Page*.

Figure 252: Custom web filter block web page.



4 Select *Override* to override the group settings for this FortiClient computer.

5 Select *Custom* for the page you want to customize and then do one of the following:

- Enter the HTML text into the text box.

or

- Select *Browse*, find the HTML file of the custom page content and select *Upload*.

6 Optionally, select *Preview* to view the custom page.

7 Select *Apply*.

Configuring antispam settings on a FortiClient computer

The antispam feature filters spam email into a special folder in the Microsoft Outlook or Outlook Express email client on the user's computer. FortiClient first checks email messages against the local black/white list and banned words list. Messages not caught in these filters are filtered using the FortiGuard AntiSpam service.

In both the black/white list and banned word filter, you can use a regular expression to create an entry that matches multiple cases.

The FortiManager unit can act as the local FortiGuard antispam service center, overriding the default FortiGuard servers. If you have a large number of FortiClient computers, using this feature speeds up the installation of the antispam settings.

To configure the antispam Black/White List

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *AntiSpam* > *Black/White List*.

4 Do any of the following:

- To remove an existing entry, select its *Delete* icon.
- To edit an existing entry, select its *Edit* icon.
- To add an entry, select *Create New*, select *Block* (black list) or *Allow* (white list), enter the email address and select *OK*.
- To copy an entry to the client group Black/White list, select its *Copy to group* icon.

To configure the banned word filter

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.
2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.
3 From the FortiClient menu, select *AntiSpam* > *Banned Word Filter*.
4 Do any of the following:

- To remove an existing entry, select its *Delete* icon.
- To edit an existing entry, select its *Edit* icon.
- To add an entry, select *Create New*, enter the banned word and select *OK*.
- To copy an entry to the client group banned word filter, select its *Copy to group* icon.

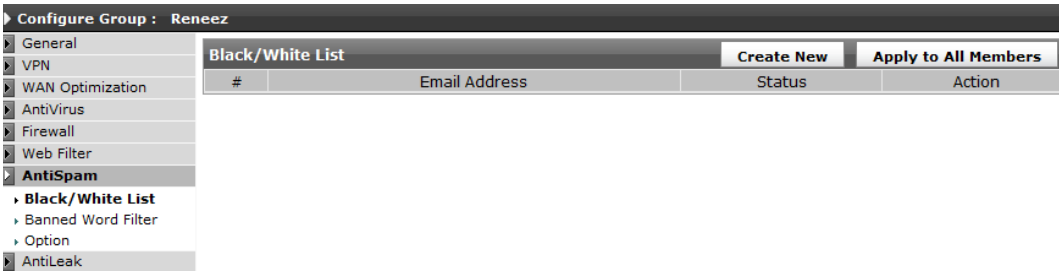
Configuring anti-spam options

You can enable anti-spam, submit mis-rated spam, and set the default anti-spam server.

To set anti-spam options

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.
2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.
3 From the FortiClient menu, select *AntiSpam* > *Option*.
4 Configure the following settings and then select *Apply*.

Figure 253: AntiSpam options.

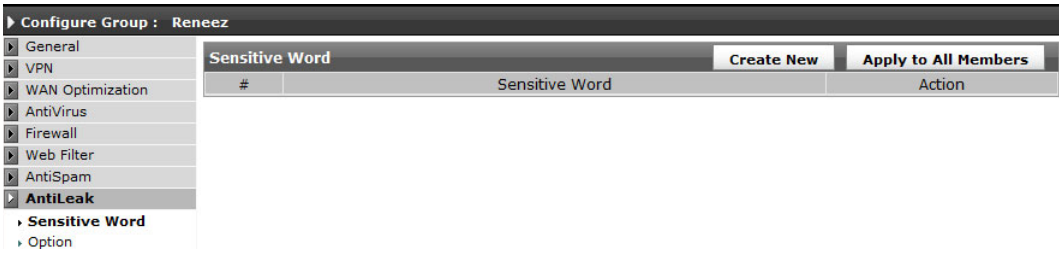


Override	The FortiClient computer's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited antispam configuration on this FortiClient computer. Deselecting override means that you want to use the configuration inherited from the group to which the computer belongs. See "Adding a FortiClient computer group" on page 320 and "Configuring settings for client groups" on page 322.
Enable Antispam	Enable the antispam feature.
Submit mis-rated Email automatically	Enable this option if you want FortiClient to automatically send mis-rated email to the Fortinet FortiGuard AntiSpam service to enhance the service's email-scanning accuracy. A user indicates an email message is mis-rated by selecting Mark Not Spam.
Don't prompt user to submit mis-rated Email	Enable this option if you do not want FortiClient to prompt users to submit mis-rated email messages to the Fortinet FortiGuard AntiSpam service. A user indicates that an email message is mis-rated by selecting Mark Not Spam. Users are also not prompted if Submit mis-rated Email automatically is enabled.
Override Default AntiSpam Server	Select to get the antispam settings from the FortiManager unit: • Enter the unit's IP address. • Enter the unit's port number.

Configuring anti-leak options on a FortiClient computer

AntiLeak prevents accidental leakage of sensitive information through email messages. When a user on a FortiClient computer sends an email message using Microsoft Outlook, FortiClient searches the attachments for the words or patterns in the AntiLeak sensitive words list. If any of the words or patterns are found, FortiMail logs the message and can also block sending of the message.

Figure 254: AntiLeak settings.



To configure the sensitive word list

1. In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.
2. In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *AntiLeak* > *Sensitive Word*.
4. Do any of the following:
   - To remove an existing entry, select its *Delete* icon.
   - To edit an existing entry, select its *Edit* icon.
   - To add an entry, select *Create New*, enter the sensitive word and select *OK*.
   - To copy an entry to the client group sensitive word list, select its *Copy to group* icon.

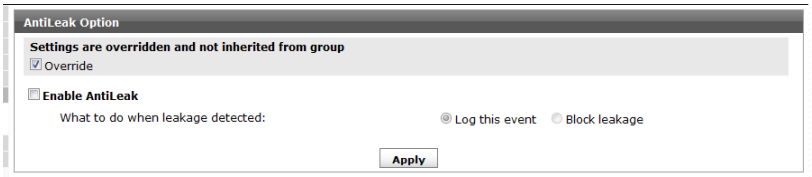
To configure AntiLeak options

1 In the FortiClient Manager, select *Client/Group* > *Client* > *Managed Client* in the Navigation Pane.

2 In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.

3 From the FortiClient menu, select *AntiLeak* > *Option*.

Figure 255: Anti-leak option



4 Select *Enable AntiLeak*.

5 Select one of the following options:

Log this event	Log outgoing email messages that leak sensitive information.
Block leakage	Block sending of email messages that leak sensitive information. Blocked messages are logged.

6 Select *Apply*.

FortiManager HA

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.

This section describes:

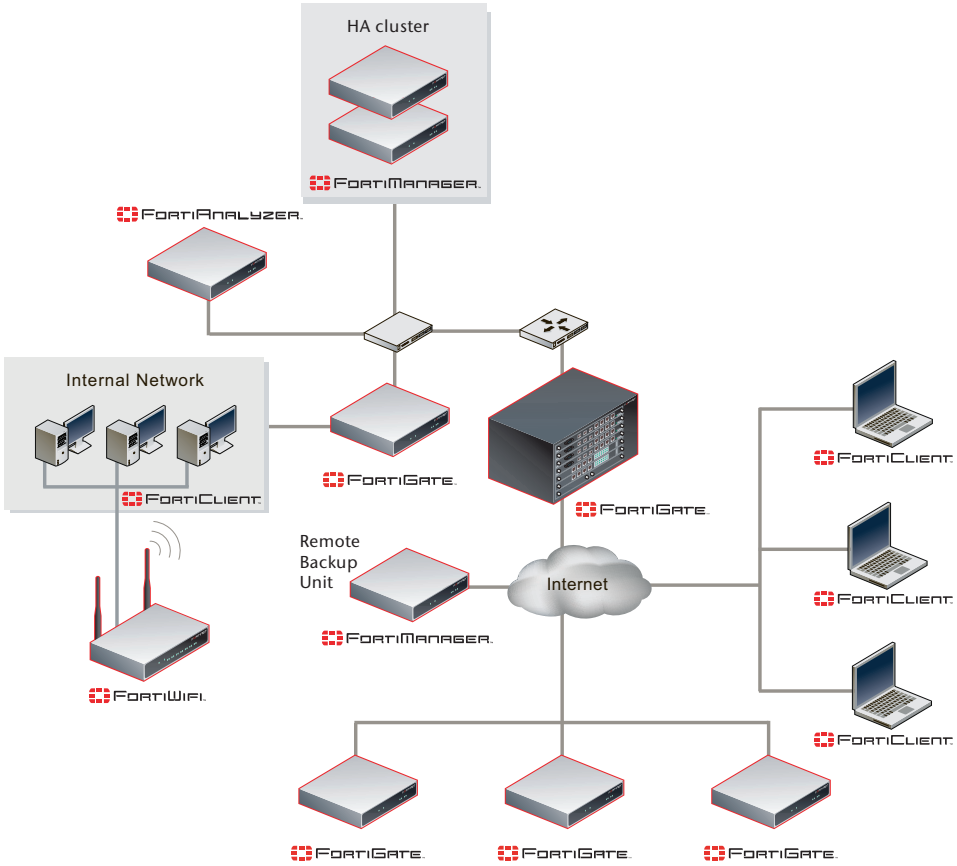
HA overview

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, FortiGate, FortiAnalyzer, FortiMail and FortiClient configuration and related information in the FortiManager database on the FortiManager unit hard disk. The Device Manager also stores and manages FortiGate firmware images and optionally FortiGuard service data 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.

Figure 256: Example FortiManager HA cluster



A FortiManager HA cluster consists of up six FortiManager units of the same FortiManager model. One of the FortiManager units in the cluster operates as a primary or master unit and the other one to five 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 web-based manager or CLI to perform FortiManager operations. The primary unit also interacts with managed FortiGate, FortiAnalyzer and FortiMail devices, and FortiClient applications. Managed devices connect with the primary unit for configuration backup and restore. If FortiManager is used to distribute firmware updates and FortiGuard updates to managed devices, the managed devices can connect to the primary 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. For the managed devices to automatically start using the new primary unit, you should add all of the FortiManager units in the cluster to the managed devices.

Note: When changing a secondary unit in an HA cluster to a primary unit, the FortiManager unit must be rebooted.

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). Also, all firmware images and all FortiGuard data stored by the Device Manager are synchronized to the backup units. 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.

Tip: 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 unit 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 real time monitor and 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.

Note: When changing a secondary unit in an HA cluster to a primary unit, the FortiManager unit must be rebooted.

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 from a peer IP address the FortiManager unit assumes the peer is functioning.

When the primary unit is receiving HA heartbeat packets from all of the configured peers or backup units, the primary unit sets the cluster status to up. Once the cluster is up the primary unit then synchronizes its configuration to the backup unit. This synchronization process can take a few minutes depending on the size of the FortiManager database. During this time database and configuration changes made to the primary unit are not synchronized to the backup units. Once synchronization is complete, if changes were made during synchronization, they are re-synchronized to the backup units.

Most of the primary unit configuration, as well as the entire FortiManager database, are synchronized to the backup unit. Interface settings and HA settings are not synchronized. These settings must be configured on each cluster unit.

Once the synchronization is complete, the FortiManager HA cluster begins normal operation.

Configuring HA options

To configure HA options go to *System Settings* > *General* > *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.

Note: When changing the HA mode for a FortiManager unit in an HA cluster, the FortiManager unit must be rebooted.

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*.

Figure 257 and Figure 258 show sample configurations for the primary and backup units in a FortiManager HA cluster.

Figure 257: Example primary unit configuration with two backup units

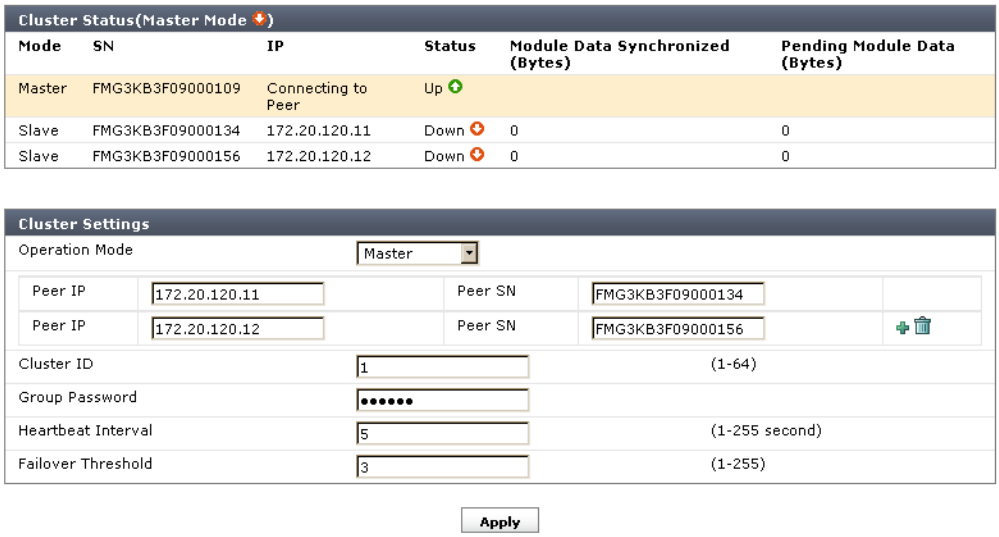
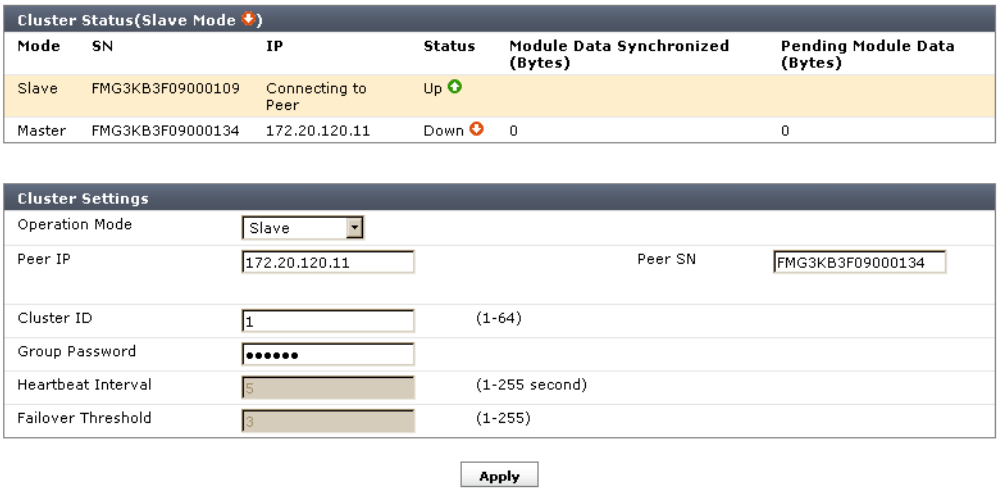


Figure 258: Example backup unit configuration



You can connect to the primary unit web-based manager 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.

Cluster Status	Monitor FortiManager HA status. See "Monitoring HA status" on page 390.
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	Enter the IP address of another FortiManager unit in the cluster. For the primary unit you can add up to five Peer IPs for up to five backup units. For a backup unit you add the IP address of the primary unit.
Peer SN	Enter the serial number of another FortiManager unit in the cluster. For the primary unit you can add up to five Peer serial numbers for up to five backup units. For a backup unit you add the serial number of the primary unit.

Group ID	A number between 0 and 64 that identifies the HA cluster. All members of the HA cluster must have the same group ID. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different group ID. The FortiManager web-based manager browser window title changes to include the Group 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.
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.

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.

Web-based manager configuration steps

Use the following procedures to configure the FortiManager units for HA operation from the FortiManager unit web-based manager.

To configure the primary unit for HA operation

1 Connect to the primary unit web-based manager.

2 Go to *System Settings* > *General* > *HA*.

3 Configure HA settings.

Operation Mode	Master
Peer IP	172.20.120.23
Peer SN	<serial_number>
Peer IP	192.268.34.23
Peer SN	<serial_number>
Group ID	15
Group Password	password
Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4 Select Apply.

5 Power off the primary unit.

To configure the backup unit on the same network for HA operation

1 Connect to the backup unit web-based manager.

2 Go to *System Settings* > *General* > *HA*.

3 Configure HA settings.

Operation Mode	Slave
Priority	5 (Keep the default setting.)
Peer IP	172.20.120.45
Peer SN	<serial_number>
Group ID	15
Group Password	password
Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4 Select Apply.

5 Power off the backup unit.

To configure a remote backup unit for HA operation

1 Connect to the backup unit web-based manager.

2 Go to *System Settings* > *General* > *HA*.

3 Configure HA settings.

Operation Mode	Slave
Priority	5 (Keep the default setting.)
Peer IP	192.168.20.23

Peer SN	<serial_number>
Group ID	15
Group Password	password
Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4 Select Apply.

5 Power off the backup unit.

To change the network configuration so that the remote backup unit and the primary unit can communicate with each other

1 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 user 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.

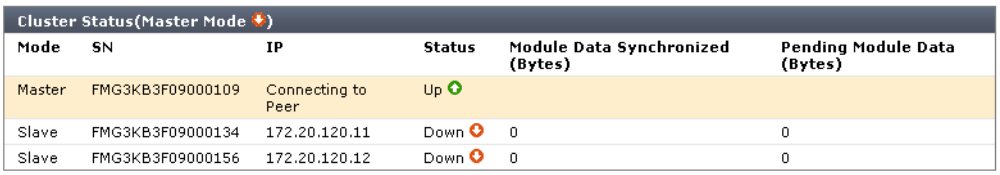
Monitoring HA status

Go to *System Settings* > *General* > *HA* and select *Status* to monitor the status of the FortiManager units in an operating HA cluster. The FortiManager HA status page displays information about the role of each cluster unit, the HA status of the cluster, and also displays the HA configuration of the cluster.

Note: The FortiManager web-based manager 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.

Note: From the FortiManager CLI you can use the command `get fmsystem ha` to display the same HA status information.

Figure 259: FortiManager HA status



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.
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.
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 FortiManager 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, and install the firmware on the primary unit web-based manager. You can also use the 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 quiet period.

To upgrade FortiManager HA cluster firmware

1. Log into the primary unit web-based manager.
2. Upgrade the primary unit firmware.
3. Log into the slave unit web-based manager.
4. Upgrade the slave unit firmware.
5. Do the same for all slave units.

Administrators may not be able to connect to the FortiManager web-based manager 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.

Managing Firmware Versions

Review this section before upgrading because it contains important information about how to properly back up your current configuration settings, including how to test the firmware before installing it permanently on your FortiManager unit.

In addition to firmware images, Fortinet releases patch releases–maintenance release builds that resolve important issues. Fortinet strongly recommends reviewing the release notes for the patch release before upgrading the firmware. Follow the steps below:

- Download and review the release notes for the patch release
- Download the patch release
- Back up the current configuration
- Install the patch release using the procedure
- Test the patch release until you are satisfied that it applies to your configuration

Installing a patch release without reviewing release notes or testing the firmware may result in changes to settings or unexpected issues.

Caution: Always back up your configuration before installing a patch release, upgrading/downgrading firmware, or resetting configuration to factory defaults.

Note: For information on backing up the FortiManager configuration, see"Backup and Restore" on page 48.

This section includes the following topics:

General upgrading information

Before upgrading your FortiManager unit, you should be aware of the following:

- Verify that your FortiManager unit is running FortiManager 3.0 MR7 Patch 3 or later; only a FortiManager unit running FortiManager 3.0 MR7 Patch 3 or later can successfully upgrade to FortiManager 4.0.
- FortiManager 4.0 supports only 3.0 MR6 and later for all devices. All device firmware must be upgraded to 3.0 MR6 or later before upgrading the FortiManager unit to FortiManager 4.0.
- If a power or network failure interrupts the upgrade process, the system may become corrupted. If the system is not accessible, re-install FortiManager 3.0 MR7 Patch 3 release or later, import the corresponding system backup configuration file and database, and then try the upgrade process again.

- The settings for the following features carry forward from FortiManager 3.0 MR7:
  - Device information and configuration
  - Group information and configuration (only some settings carry forward)
  - Revision History (using import/export functions)
  - Scripts
  - Service
  - Firmware
  - System Settings (only some settings carry forward.

The sequential order of the following ensures a successful upgrade and should always be followed in this order. If you want to restore the global database and configuration, restore after step 6 is complete.

1. Save any pending configurations and back up all configuration, including all devices' configurations as well. The device database is not carried forward.
2. If not done so already, upgrade the devices' firmware to 3.0 MR6 or higher. Use the procedure in "Upgrading a FortiGate device or group" on page 397.
3. Verify that your FortiManager firmware is running FortiManager 3.0 MR7 Patch 3 or later. If not back up your current configuration (including all devices' configuration) and upgrade to FortiManager 3.0 MR7 Patch 3 or later.
4. Upgrade the FortiManager unit to FortiManager 4.0 MR2.
5. View the settings that carried forward and verify what has or has not carried forward.
6. Review your scenario to determine which mode your FortiManager unit should be in, either EMS Mode or GMS Mode.

Upgrading your FortiManager unit

You may need to reconfigure some configuration settings in FortiManager 4.0 MR2 after upgrading. See "General upgrading information" on page 393 for which configuration settings are carried forward.

You can also use the following procedure when installing a patch release. A patch release is a firmware image that resolves specific issues without containing new features and/or changes to existing features. You can install a patch release whether you upgraded to the current firmware version or not.

Fortinet recommends using the CLI to upgrade to FortiManager 4.0 MR2. The CLI upgrade procedure reverts all current firewall configurations to factory default settings.

Upgrading to FortiManager 4.0 MR2 through the web-based manager

Caution: Always back up your configuration before installing a patch release, upgrading/downgrading firmware, or resetting configuration to factory defaults..

The following procedure uses the web-based manager for upgrading to FortiManager 4.0 MR2.

The following procedure assumes that you have already downloaded the firmware image to your management computer.

To upgrade to FortiManager 4.0 MR2 through the web-based manager

1. Copy the firmware image file to your management computer.

2 Log in to the web-based manager.

3 Go to *System Settings> General* > *Firmware Update* if you are upgrading from v4.0 or 4.0 MR1 or *System Settings* > *Maintenance* > *Firmware Upgrade* if you are upgrading from v3.0.

4 Select *Upgrade Server Image*, then *Next.*

5 Select *Browse* and locate the image file on you local computer.

6 Select *Finish*.

The FortiManager server installs the file and restarts, running the new version of the firmware. The FortiManager unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiManager login. This process may take a few minutes.

If you need to restore the FortiManager global database after the upgrading, use the following procedure.

To restore the FortiManager global database configuration

1 Log in to the web-based manager.

2 Go to *Device Manager* > *Script* > *CLI Script*.

3 Select *Create New*.

4 Enter a name for the configuration file that you are restoring.

5 Copy and paste the exported database and configuration file you created.

6 Select *OK*.

7 In Script, select *Run on Global Database* icon.

8 Select *View Log* to review the execution history and result.

Upgrading to FortiManager 4.0 through the CLI

The following procedure uses the CLI to upgrade to FortiManager 4.0 MR2 and a TFTP server. The CLI upgrade procedure reverts all current firewall configurations to factory default settings.

The following procedure assumes that you have already downloaded the firmware image to your management computer.

Fortinet recommends using the CLI to upgrade to FortiManager 4.0 MR2. The CLI upgrade procedure reverts all current firewall configurations to factory default settings.

To upgrade to FortiManager 4.0 through the CLI

1 Copy the new firmware image file to the root directory of the TFTP server.

2 Start the TFTP server.

3 Log in to the CLI.

4 Enter the following command to ping the computer running the TFTP server:

```
execute ping <server_ipaddress>
```

Pinging the computer running the TFTP server verifies that the FortiManager unit and TFTP server are successfully connected.

5 Enter the following to restart the FortiManager unit.

```
execute reboot
```

6 As the FortiManager unit reboots, a series of system startup messages appears. When the following message appears:

```
Press any key to display configuration menu
```

7 Immediately press any key to interrupt the system startup. You have only three seconds to press any key. If you do not press a key soon enough, the FortiManager unit reboots and you must log in and repeat steps 5 to 7 again.

8 If you successfully interrupt the startup process, the following message appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
```

9 Type `G` to get the new firmware image from the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

10 Type the address of the TFTP server and press *Enter*.

The following message appears:

```
Enter Local Address [192.168.1.188]:
```

11 Type the internal IP address of the FortiManager unit.

This IP address connects the FortiManager unit to the TFTP server. This IP address must be on the same network as the TFTP server, but make sure you do not use an IP address of another device on the network. The following message appears:

```
Enter File Name [image.out]:
```

12 Enter the firmware image file name and press *Enter*.

13 The TFTP server uploads the firmware image file to the FortiManager unit and the following message appears:

```
Save as Default firmware/Backup firmware/Run image without
saving: [D/B/R]
```

14 Type `D`.

15 After system reboots, reconfigure system settings.

Verifying the upgrade

When the upgrade is successfully installed:

- ping to your FortiManager unit to verify there is still a connection
- clear the browser's cache and log into the web-based manager

After logging back in to the web-based manager, certain configuration settings from FortiManager 3.0 MR7 Patch 3 or later should have carried forward; verify that they have using the list in "General upgrading information" on page 393.

You should verify what configuration settings carried forward. You should also verify that administrative access settings carried forward as well. Verifying your configuration settings enables you to familiarize yourself with the new features and changes in FortiManager 4.0 MR2.

You can verify your configuration settings by:

- going through each menu and tab in the web-based manager

- using the `show` shell command in the CLI.

Upgrading a FortiGate device or group

Caution: Always back up your configuration before installing a patch release, upgrading/downgrading firmware, or resetting configuration to factory defaults.

You need to upgrade your FortiGate device or group when there is a new firmware version or maintenance release for the FortiManager unit. You can immediately change a FortiGate device or group's firmware, or you can schedule a change in the future. For example, you might update firmware during the night when there is less traffic on your network.

The following procedures can also be used to downgrade a FortiGate device or group.

The following procedure assumes that you have already downloaded the firmware image to your management computer.

To upgrade a FortiGate device or group

1. Go to *Device Manager* > *Device Name* if you are upgrading a device, or *Device Manager* > *Device Group Name* if you are upgrading a device group.
2. Select a FortiGate device or group.

   Firmware change schedules are separate at the group and device level.
3. Go to *System* > *Status* > *Firmware*.
4. To install the firmware immediately, click *Upgrade Now* and click *OK*.

   The FortiManager unit attempts to upgrade the FortiGate unit immediately; time varies by model and speed of the connection.
5. To install the firmware in the future, select *Schedule Upgrade*. The Firmware Upgrade/Downgrade window opens.
6. If your FortiGate device has a partition, and you want to upgrade the FortiGate unit using that partition, select the *Boot From Alternate Partition After Upgrade* check box.
7. Enter the date and time you want to schedule the upgrade.
8. If the upgrade fails, select one of the following options:
   - Select *Cancel Upgrade* if you want to cancel if it is unsuccessful
   - Select *Retry* and enter the number and interval for retry attempts.
9. Click *OK*.
-

Canceling a scheduled firmware upgrade

You can cancel scheduled firmware changes for a FortiGate device or group that have not started yet; however, you cannot cancel firmware changes that:

- have already been tried at least once and are configured to retry ***n*** times
- are currently in progress

To cancel a scheduled upgrade or downgrade schedule

1. Go to *Device Manager* > *Device Name* > *System* > *Status* > *Firmware or Device Manager* > *Device Group Name* > *System* > *Status* > *Firmware* if you are upgrading a device group.

   If firmware changes have been scheduled at both the group and the device level, you will need to clear each schedule separately.
2. In the row corresponding to the scheduled firmware change, click *Delete*.

   If you have scheduled more than one upgrade, you may need to click *Delete* multiple times to completely clear the schedule.

•

Index

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W