FortiManager v5.0 Patch Release 2

Administration Guide

FortiManager v5.0 Patch Release 2 Administration Guide

April 22, 2013

02-502-184107-20130422

Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Table of Figures

Change Log

Date	Change Description
2012-10-30	Initial release.
2013-04-09	Updated for FortiManager v5.0 Patch Release 2.
2013-04-10	Updated HA firmware instructions.
2013-04-22	Updated available device tabs list.

Introduction

FortiManager centralized management appliances deliver the essential tools needed to effectively manage your Fortinet-based security infrastructure.

Using the FortiManager system, you can:

- configure multiple FortiGate units (including FortiGate, FortiWiFi, FortiGate VM), FortiCarrier units, and FortiSwitch units,
- segregate management of large deployments easily and securely by grouping devices into geographic or functional administrative domains (ADOMs),
- configure and manage VPN policies,
- monitor the status of managed devices,
- view device logs and generate reports with integrated FortiAnalyzer features,
- update the antivirus and attack signatures,
- update vulnerability and compliance management updates,
- provide web filtering and email filtering services to the licensed devices as a local FortiGuard Distribution Server (FDS).
- revision control and firmware images management of managed devices.

FortiManager systems scale to manage up to 10 000 devices and virtual domains (VDOMS) from a single FortiManager interface. FortiManager is designed for medium to 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 this document
- FortiManager documentation

About this document

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

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

FortiManager documentation

The following FortiManager product documentation is available:

- *FortiManager v5.0 Patch Release 2 Administration Guide*

  This document describes how to set up the FortiManager system and use it to manage supported Fortinet units. It includes information on how to configure multiple Fortinet units, configuring and managing the FortiGate VPN policies, monitoring the status of the managed devices, viewing and analyzing the FortiGate logs, updating the virus and attack signatures, providing web filtering and email filter service to the licensed FortiGate units as a local FortiGuard Distribution Server (FDS), firmware revision control and updating the firmware images of the managed units.

- *FortiManager System QuickStart Guides*

  These documents are included with your FortiManager system package. Use these document to install and begin working with the FortiManager system and FortiManager 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 v5.0 Patch Release 2 CLI Reference*

  This document describes how to use the FortiManager Command Line Interface (CLI) and contains references for all FortiManager CLI commands.

- *FortiManager v5.0 Release Notes*

  This document describes new features and enhancements in the FortiManager system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.

- *FortiManager v5.0 Patch Release 2 Log Message Reference*

  This document describes the structure of FortiManager log messages and provides information about the log messages that are generated by the FortiManager system.

What's New in FortiManager v5.0.2

This chapter lists and describes some of the key changes and new features available in FortiManager v5.0 Patch Release 2.

This following topics are discussed:

- Device Manager tab
- Policy & Objects tab
- System Settings tab
- Reports tab
- Advanced features improvements
- Other improvements

Device Manager tab

The following improvements and changes have been made to the *Device Manager* tab:

- Log arrays
- Device manager layout
- Policy package status
- Device profiles
- Extend workspace to entire ADOM
- Quick install

Log arrays

Log arrays have been added to support group-based access to logs and reports. Log arrays are available in the *Device Manager* tab under the *Devices & Groups* menu. Log arrays also allow you to manage log data belonging to FortiGate HA clusters from a single device object. You can configure RTM profiles and schedule reports for each log array. See "Log arrays" on page 148 for more information.

Device manager layout

The *Device Manager* tab now has collapsed ADOM navigation, where all of the ADOMs are displayed on the tree-menu. Unlike FortiManager v4.0 MR3, you do not need to enter each ADOM individually. See "Device Manager tab" on page 114 for more information.

The *Device Manager* tab has the following changes:

- The *All FortiGate* and *All FortiCarrier* device groups are displayed under each ADOM
- Device profiles are available under a separate heading on the tree-menu
- The number of devices is displayed in parentheses next to each device group name

- The *All FortiSwitch* device group is displayed in a separate, dedicated ADOM at the bottom of the tree-menu.
- Script and web portal features are disabled by default. You can enable these advanced configuration options under *System Systems* > *Admin* > *Admin Settings*. Select *Show Script* and *Show Web Portal* to enable on these options.

The content pane has two possible views: horizontal and vertical.

There is a quick filter option available in vertical view to quickly find devices in certain states including *Connection Down, Config Changed,* and *License Expired.* The Web-based Manager will remember the state of the quick filter when returning to the *Device Manager* tab. Filters in the horizontal view are set per column.

You can select the preferences button to change the view-mode between horizontal and vertical views.

Horizontal view

In the horizontal view, the top portion of the content pane shows the device list. When you select one of the devices in the table, the bottom portion of the content pane displays the selected device’s dashboard. The menu navigation of the device settings is changed to a tab format, the dashboard toolbar. See “Horizontal view” on page 116 for more information.

If ADOMs are enabled, the navigation pane icons *Install*, *Add device*, and *Add Group* are hidden. You can use the right-click context menus within an ADOM to launch the *Add Device* and *Install* wizards, and perform other menu actions.

If the administrator hovers their cursor over an ADOM, information will be displayed about that ADOM including the ADOM version, mode, and VPN management options.

Vertical view

In the vertical view, devices are displayed on a vertical list on the left side of the content pane. See “Vertical view” on page 116 for more information.

Edit a group

An administrator can right-click on a group to quickly edit, add, or delete devices/VDOMs that belong to the group.

ADOM properties

ADOMs can be edited to change properties and to add devices or VDOMs to the ADOM.

ADOM properties include:

- Name
- Version
- Mode (Normal | Backup)
- VPN Management (Central VPN Console | Policy & Device VPNs)
- Lock ADOM
- Devices/VDOMs

Quick filter

A quick filter is available in both modes to allow you to find devices in certain states.

Device dashboard

An icon has been added to the *Configuration and Installation Status* widget for when a device is synchronized, but the configuration was retrieved from the device (e.g. modifications were made directly on the FortiGate and synced to the FortiManager). A tool tip will show the last date and time that the synchronization occurred.

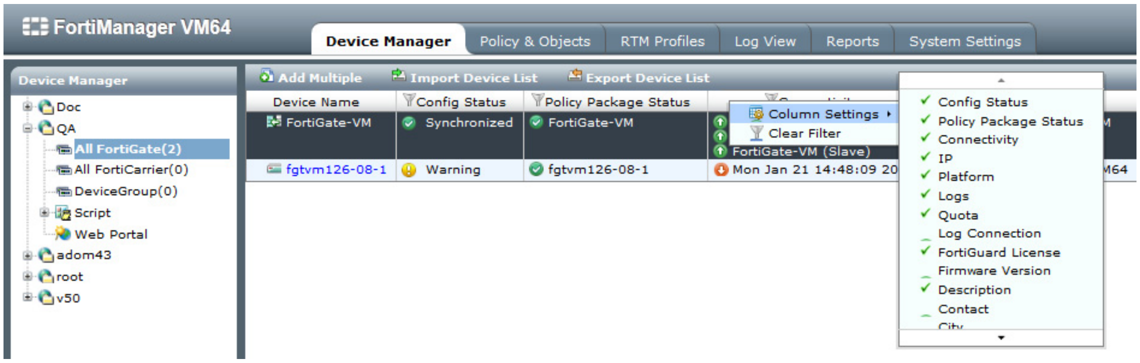
The widgets have changed as follows:

- *Unit Operation* widget has been removed.
- *System Information* widget:
  - Added *[Change]* to HA Mode and launch HA dialog
  - Added a field to reboot or shutdown the unit
- *License Information* widget
  - Under *FortiGuard Services* added *Update Frequency: Daily [Change]*
  - *[Change]* launches the FortiGuard configuration page.

Policy package status

To view the policy package status, right-click on the content pane, select *Column Settings*, and then select *Policy Package Status* in the pop-up menu. When you hover the mouse cursor over the column icon, you can see when the last check was performed. When the admin makes a change to any policies, the corresponding policy package will be deemed *dirty*, and will show as such in the device list.

Figure 1: Column settings



Device Name	Config Status	Policy Package Status	
FortiGate-VM	Synchronized	FortiGate-VM	FortiGate-VM (Slave)
fgtvm126-08-1	Warning	fgtvm126-08-1	Mon Jan 21 14:48:09 20

From *Column Settings*, you can choose to display the following information:

Config Status	Platform	FortiGuard License	City
Policy Package Status	Logs	Firmware Version	Province
Connectivity	Quota	Description	Country
IP	Log Connectivity	Contact	Company

Device profiles

A device profile is a subset of a model device configuration. Each device or device group will be able to be linked with a device profile. When linked, the selected settings will come from the profile, not from the *Device Manager* database. See "Device profiles" on page 147 for more information.

By default, there is one generic profile defined. Device profiles are managed in a similar manner to policy packages. You can use the context menus to create new device profiles.

Device profiles will support the following settings:

- DNS: Networking options including DNS servers and local domain name
- Time settings: NTP server settings
- Alert Email: Configure SMTP server settings
- Admin Settings: Configure central management, web administration ports, timeout settings, and other web administration settings.
- SNMP: Configure SNMPv1, v2c and v3 settings.
- Replacement messages: Customize replacement messages at a global level. You can customize per VDOM replacement messages.
- Log Settings: Configure logging and archiving to FortiAnalyzer/FortiManager or a syslog server.

You can create or delete profiles with a context menu by right-clicking the profile. You can also select specific devices that will be associated with the profile. You can link a device to the device profile using the *Add Device Wizard* from the device’s dashboard in device manager, or by right-clicking and editing the profile and selecting the devices.

Installation considerations

Device profiles should be applied to a device (database) during the install operation. There are three types of installations:

- *Device Settings only*: the device profile should be applied first.
- *Policy Packages and Device Settings*: the device profile make be applied after the policy package is copied.
- *Interface Policy only*: the device profile should be applied in the same way as other global settings are handled, depending on whether or not VDOMs are enabled.

During the installation wizard, you will be prompted to choose which devices to install. After selecting device settings only, you will be presented with a list of devices that is pre-filtered based on whether or not the device database is modified.

Extend workspace to entire ADOM

When concurrent ADOM access is enabled, administrators are able to lock and unlock ADOM access using a right-click menu option that has been added. The ADOM lock status is displayed by a lock icon to the left of the ADOM name. The lock status is as follows:

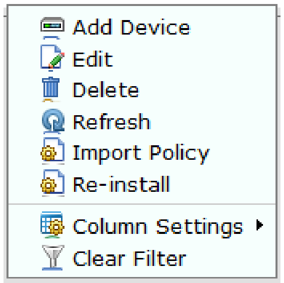
- Grey lock: The ADOM is currently unlocked, and is read/write.
- Green lock: The ADOM is locked by you when logged in as an admin.
- Red lock: The ADOM is locked by another admin.

An additional CLI command has been added under `config system global` to enable or disable ADOM lock override: `set lock-preempt {enable | disable}`. When the ADOM lock override is enabled, if two administrators are concurrently accessing an ADOM and one attempts to lock the ADOM, the other administrator can kick the administrator off of the ADOM, preventing the ADOM from being locked.

Quick install

You can right-click on the *Policy Config Status* column icon to perform a quick reinstallation of a policy package without launching the *Install Wizard*. The content menu is disabled when the policy package is already in synchronization. You can also right-click on *Config Status* if the device is out of synchronization to install any device setting changes. This will only affect the settings for the selected device. In FortiManager v5.0 Patch Release 2 you can perform a quick install for multiple devices. See "Quick install" on page 119 for more information.

Figure 2: Reinstall a policy package without launching the install wizard



Policy & Objects tab

The following improvements and changes have been made to the Policy & Objects tab:

- Bind zone to an address
- Policy & Objects dual pane

See "Policy & Objects" on page 209 for more information.

Bind zone to an address

Similar to FortiOS interface binding for addresses, FortiManager now supports binding a zone to an address when creating address objects at both the global and ADOM level. Once bound to a zone, the address will only be available for selection when the appropriate zone is selected for a policy.

Policy & Objects dual pane

The *Policy & Objects* tab has been redesigned to create a dual pane layout. The ADOM related objects appear on the bottom pane, and the top pane contains the policies for the selected policy package.

You can drag and drop one or more objects from the object frame into a specific cell of the policy, for example, drag and drop an address to the source or destination cell of the policy.

The following features are available for drag and drop:

- Drag one or more objects without opening a new page
- Edit objects while keeping the policy table in view
- Highlighted permitted cell targets
- Previously selected objects remain highlighted in the object list until the drag operation completed.

Web-based Manager improvements have been made to the policy table. See "Display Options" on page 213 for more information.

Policy package

You can create the following types of local domain policies/identity policies:

- Policy
- Central NAT
- IPv6 Policy
- DOS Policy

See “Managing policy packages” on page 213 for more information.

Objects

Configurable objects include the following:

- Zone
- Firewall Objects
- UTM Objects
- User & Device
- WAN Opt
- Dynamic Objects
- CA Certificates
- Tag Management

See “Managing objects and dynamic objects” on page 222 for more information.

System Settings tab

Changes to the *System Settings* tab to improve the granularity of policy packages. See “System Settings” on page 48 for more information.

Policy package granularity

Admin profiles can be configured at both the global and ADOM scope. Profile configuration has become more granular. You can now specify whether or not an admin profile read-write, read-only, or no access for various global, ADOM, and other settings including policy packages and policy objects.

Global settings

- System Settings
- Administrator Domain
- Global Policy Packages
- Global Objects
- Assignment

ADOM settings

- Add/Delete Devices/Groups
- Install to Devices
- Retrieve Configuration from Devices
- Terminal Access

- Consistency Check
- Device Manager
- Manage Device Configuration
- Policy Package
- Policy Objects
- VPN Manager

Other settings

- Real Time Monitor
- Log Viewer
- Report Viewer

New administrators

When creating a new administrator, you can assign a default or custom administrator profile, and specify ADOM and policy package access. See "Administrator" on page 80 for more information.

Reports tab

FortiManager now includes an SQL-based *Reports* tab, similar to FortiAnalyzer. See "Reports" on page 252 for more information. Highlights of this tab include the following:

- Device manager layout
- Report schedule
- Report history
- Report calendar
- Advanced

Report templates

Go to the *Reports* tab on the right pane to view report templates and other configuration options. On this page you can configure reports using the pre-defined report templates or right-click on the navigation tree to create a new template. See "Templates" on page 253 for more information.

Go to *Reports* > *[ADOM]* > *Report Templates*, to configure report templates and to view report calendars. Two pre-defined report templates are included: Client Reputation and UTM Security Analysis. Use the right-click menu on the tree menu to create a new template or report schedule, and to view historical reports.

Use the icons on the right pane to sections to a report which can be displayed with a page break between each other. You can configure the section to show either one or two columns and set a section title to each column.

Select the *Edit* icon to customize charts on the report template. The charts are organized into the following categories: Event, IPS (Attack), Network Scan, Traffic, Virus, and Web Filter.

You can drag and drop template elements to further customize the report layout.

Report schedule

You can create schedules for reports and view the schedule either as a list or in calendar format. You can download any previously generated reports from either the list view or calendar view. See “Schedules” on page 259 for more information.

Report history

Historical Reports allows you to view all reports that have been generated on the FortiManager system. It displays the report name, date and time that the report was generated, and the device type. See “History” on page 262 for more information.

Report calendar

Report Calendar provides an overview of report schedules. You can view all reports scheduled for the selected month. You can left-click on any day on the calender to create a new report schedule. When hovering the mouse cursor over a scheduled report on the calendar, a notification box will appear detailing the report name, status and device type. Left-click a completed schedule to save the report as a PDF to your hard drive. *Calendar* is useful for managing report generation. See “Calendar” on page 264 for more information.

Advanced

The *Advanced* section allows you to view and configure charts, datasets, output profiles, and languages. See “Advanced” on page 265 for more information.

Advanced features improvements

JSON API improvements

The following improvements have been made to the JSON API:

- Support full database configuration API
- Support API extensions for Real-Time Monitor
- Support API extensions for Log View
- Added API to check FortiManager high availability status
- Updated API for Security Console and DVM

Script Web-based Manager

The organization of scripting has been improved in the Web-based Manager. It now includes the following improvements:

- By default, scripting is hidden and disabled in the *System Settings* tab
- Separate enable options have been added for *Script Grouping*, *Automatic Scripts*, and *TCL Scripts*
- The script node has been flattened to a single page.
- The CLI can be run from the scripting page
- Right-click menus provide additional options
- Users can create scripts based on the current database

- By default, filters and other options are hidden
- The script history page has been improved.

See “Scripting” on page 196 for more information.

Web portal developer SDK improvements

A new Web Portal Developer tools site has been created. This site is restricted to customers that have purchased the SDK SKU, and will host all of the SDK materials. See “Configuring web portals” on page 202 for more information.

XML API improvements

The following improvements have been made to the XML API:

- Support for global zone mapping extension.
- New function added; `getSystemStatus`.

Other improvements

High Availability takeover without reboot

In FortiManager v4.0 MR3, when a HA slave was promoted a reboot was required, This behavior has changed so that a reboot is not required when the slave is promoted to master. See “High Availability” on page 297 for more information.

IPv6 administration

Administrators can log in over IPv6 for HTTP, HTTPS, SSH, and Telnet.

Single interface zones

An extension to the global zone feature, Single Interface zones are designed to minimize user errors during setup for handling Virtual IP, and other configurations.

This feature has two parts:

- For each global zone, there is an option for a single interface zone.
- When defining a Virtual IP, any type of global zone can be selected as mapping.

  When Single Interface Zone is selected, the FortiManager can simply install configurations directly to the FortiGate without the need to create a new zone on FortiGate side.

If a non-single-interface zone is selected, the user will need to create a mapping for a Dynamic Virtual IP on the FortiGate device.

Fortinet Management Theory

FortiManager is an integrated platform for the centralized management of products in a Fortinet security infrastructure. A FortiManager provides centralized policy-based provisioning, configuration and update management for FortiGate (including FortiGate, FortiWiFi, and FortiGate VM), FortiCarrier, and FortiSwitch devices.

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

The FortiManager scales to manage up to 10 000 devices and virtual domains (VDOMs) from a single FortiManager interface. It is primarily designed for medium to large enterprises and managed security service providers.

Using a FortiManager device as part of an organization's Fortinet security infrastructure can help minimize both initial deployment costs and ongoing operating expenses. It allows fast device provisioning, detailed revision tracking, and thorough auditing.

Key features of the FortiManager system

Configuration revision control and tracking

Your FortiManager unit records and maintains the history of all configuration changes made over time. Revisions can be scheduled for deployment or rolled back to a previous configuration when needed.

Centralized management

FortiManager can centrally manage the configurations of multiple devices from a single console. Configurations can then be built in a central repository and deployed to multiple devices when required.

Administrative domains

FortiManager can segregate management of large deployments by grouping devices into geographic or functional ADOMs.

Local FortiGuard service provisioning

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

Firmware management

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

Scripting

FortiManager supports CLI or TCL based scripts to simplify configuration deployments.

Logging and reporting

FortiManager can also be used to log traffic from managed devices and generate SQL-based reports. FortiManager also integrates FortiAnalyzer logging and reporting features.

Fortinet device life cycle management

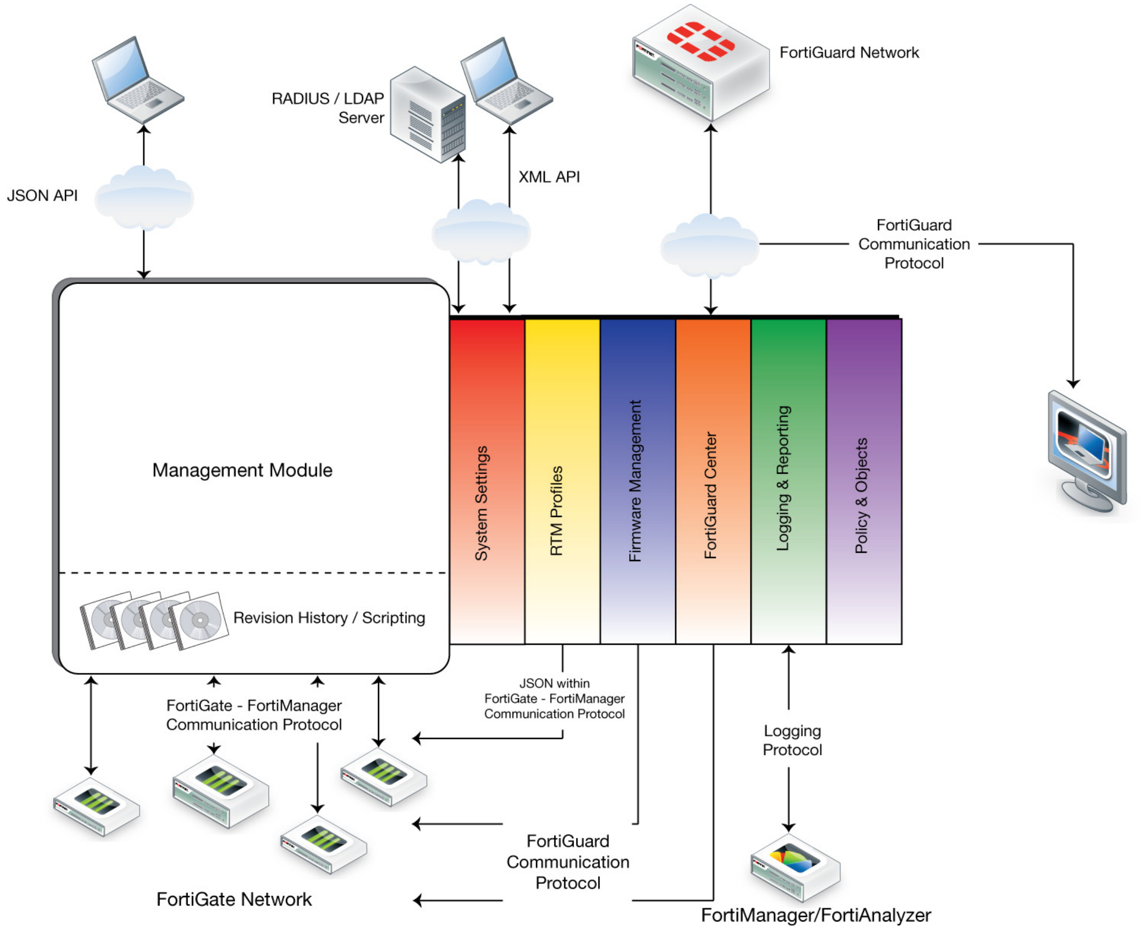
The management tasks for devices in a Fortinet security infrastructure follow a typical life cycle:

- ***Deployment***: An administrator completes configuration of the Fortinet devices in their network after initial installation.
- ***Monitoring***: The administrator monitors the status and health of devices in the security infrastructure, including resource monitoring and network usage. External threats to your network infrastructure can be monitored and alerts generated to advise.
- ***Maintenance***: The administrator performs configuration updates as needed to keep devices up-to-date.
- ***Upgrading***: Virus definitions, attack and data leak prevention signatures, web and email filtering services, and device firmware images are all kept current to provide continuous protection for devices in the security infrastructure.

Inside the FortiManager system

FortiManager is a robust system with multiple layers to allow you to effectively manage your Fortinet security infrastructure.

Figure 3: FortiManager conceptual diagram


FortiGuard Network
RADIUS / LDAP Server
XML API
JSON API
FortiGuard Communication Protocol
Management Module
Revision History / Scripting
System Settings
RTM Profiles
Firmware Management
FortiGuard Center
Logging & Reporting
Policy & Objects
FortiGate - FortiManager Communication Protocol
JSON within FortiGate - FortiManager Communication Protocol
Logging Protocol
FortiGuard Communication Protocol
FortiGate Network
FortiManager/FortiAnalyzer

Device Manager tab

The *Device Manager* tab contains all ADOMs, and devices. You can create new ADOMs, device groups, provision and add devices, install policy packages and device settings.

Policy & Objects tab

The *Policy & Objects* tab contains all of your global and local policy packages and objects that are applicable to all ADOMs, and configuration revisions.

System Settings tab

The *Systems Settings* tab enables the configuration of system settings and monitors the operation of your FortiManager unit.

RTM Profiles tab

The real-time monitor is used to view the live status of managed devices to identify trends, outages or other events that may require your attention. Where an administrator would normally log on to each individual device to view system resources and information, they can view that information from the real-time monitor on the FortiManager unit.

Log View tab

The *Log View* tab provides log configuration options and detailed logging information which can be exported and viewed.

Reports tab

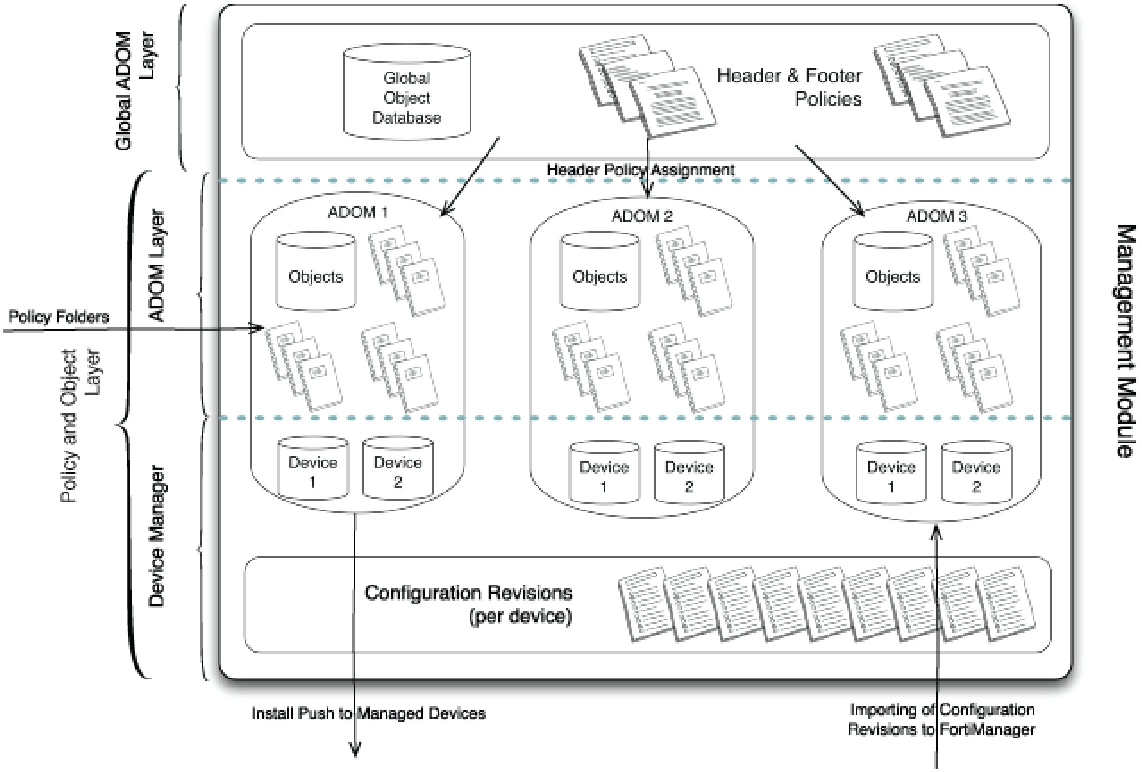
The *Reports* tab provides detailed SQL-based reporting of managed devices.

FortiGuard Center

Service updates and lookups are provided through the FortiGuard Distribution Network (FDN). The FDN is a global network of FortiGuard Distribution Servers (FDS) providing current antivirus and IPS engines and signatures, web filtering and email filter rating databases and lookups, and firmware images. If you deploy your FortiManager unit to be a private FDS, the FortiManager unit will synchronize available updates with the FDN, then provide FortiGuard updates to your managed devices. Using a private FDS provides a faster connection to your security infrastructure.

Inside the FortiManager device manager tab

Figure 4: Management model



Global ADOM layer

The global ADOM layer contains two key pieces: the global object database and all header and footer policies.

Header and footer policies are used to envelop policies within each individual ADOM. These are typically invisible to users and devices in the ADOM layer. An example of where this would be used is in a carrier environment, where the carrier would allow customer traffic to pass through their network but would not allow the customer to have access to the carrier's network assets.

ADOM layer

The ADOM layer is where the FortiManager manages individual devices or groups of devices. It is inside this layer where policy packages and folders are created, managed and installed on managed devices. Multiple policy packages can be created here, and they can easily be copied to other ADOMs to facilitate configuration or provisioning of new devices on the network. The ADOM layer contains one common object database per ADOM, which contains information such as addresses, services, antivirus and attack definitions, and web filtering and email filter.

Device manager layer

The device manager layer records information on devices that are centrally managed by the FortiManager unit, such as the name and type of device, the specific device model, its IP address, the current firmware installed on the unit, the device's revision history, and its real-time status.

Using the Web-based Manager

This section describes general information about using the Web-based Manager to access the Fortinet system from within a current web browser.

This section includes the following topics:

- System requirements
- Connecting to the Web-based Manager
- Web-based Manager overview
- Configuring Web-based Manager settings
- Reboot and shutdown of the FortiManager unit

Additional configuration options and short-cuts are available using the right-click menu. Right-click the mouse on different navigation panes on the Web-based Manager page to access these options.

System requirements

Supported web browsers

The following web browsers are supported by FortiManager v5.0 Patch Release 2:

- Internet Explorer version 9
- Firefox version 18

Other web browsers may function correctly, but are not supported by Fortinet.

Monitor settings for Web-based Manager access

Fortinet recommends setting your monitor to a screen resolution of 1280x1024. This allows for all the objects in the Web-based Manager to be viewed properly.

Connecting to the Web-based Manager

The FortiManager unit can be configured and managed using the Web-based Manager or the CLI. This section will step you through connecting to the unit via the Web-based Manager.

To connect to the Web-based Manager:

1. Connect the Port 1 interface of the unit to a management computer using the provided Ethernet cable.
2. Configure the management computer to be on the same subnet as the internal interface of the FortiManager unit:
   a. Browse to *Network and Sharing Center* > *Change Adapter Settings* > *Local Area Connection Properties* > *Internet Protocol Version 4 (TCP/IPv4) Properties*.
   b. Change the IP address of the management computer to `192.168.1.2` and the netmask to `255.255.255.0`.
3. To access the FortiManager unit's Web-based Manager, start an internet browser of your choice and browse to `https://192.168.1.99` (remember to include the "s" in https://).
4. Type admin in the *Name* field, leave the *Password* field blank, and select *Login*.

You can now proceed with configuring your FortiManager unit.

If the network interfaces have been configured differently during installation, the URL and/or permitted administrative access protocols (such as HTTPS) may no longer be in their default state.

For information on enabling administrative access protocols and configuring IP addresses, see "Configuring network interfaces" on page 71.

If the URL is correct and you still cannot access the Web-based Manager, you may also need to configure static routes. For details, see "Configuring static routes" on page 72.

Web-based Manager overview

FortiManager v5.0 Patch Release 2 introduces an improved Web-based Manager layout and tree menu for improved usability. For more information, see "What's New in FortiManager v5.0.2" on page 18.

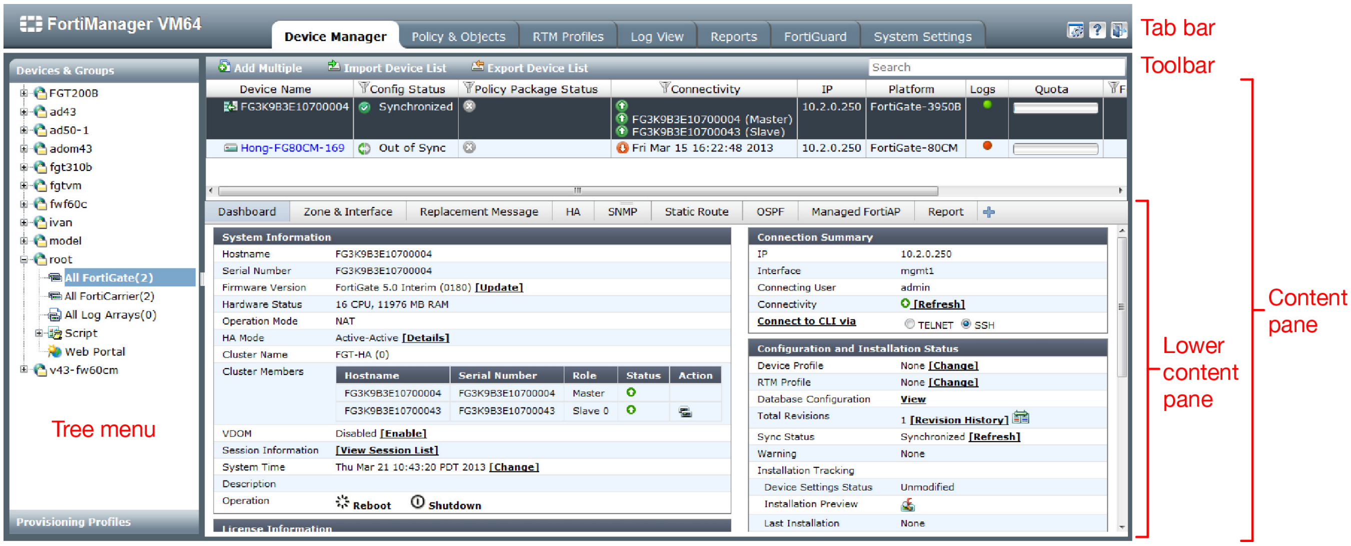
This section describes the following topics:

- Viewing the Web-based Manager
- Using the navigation pane

Viewing the Web-based Manager

The default Web-based Manager view is horizontal view. All FortiManager modules can be viewed in the horizontal view. The four main parts of the FortiManager Web-based Manager are the tree menu, navigation pane, toolbar, and right content pane.

Figure 5: Web-based Manager horizontal view



Device Name	Config Status	Policy Package Status	Connectivity	IP	Platform	Logs	Quota
FG3K9B3E10700004	Synchronized		FG3K9B3E10700004 (Master) FG3K9B3E10700043 (Slave)	10.2.0.250	FortiGate-3950B	●	
Hong-FG80CM-169	Out of Sync		Fri Mar 15 16:22:48 2013	10.2.0.250	FortiGate-80CM	●	

System Information

Hostname	FG3K9B3E10700004
Serial Number	FG3K9B3E10700004
Firmware Version	FortiGate 5.0 Interim (0180) **[Update]**
Hardware Status	16 CPU, 11976 MB RAM
Operation Mode	NAT
HA Mode	Active-Active **[Details]**
Cluster Name	FGT-HA (0)
Cluster Members	

Hostname	Serial Number	Role	Status	Action
FG3K9B3E10700004	FG3K9B3E10700004	Master	✓	
FG3K9B3E10700043	FG3K9B3E10700043	Slave 0	✓	

VDOM	Disabled **[Enable]**
Session Information	**[View Session List]**
System Time	Thu Mar 21 10:43:20 PDT 2013 **[Change]**
Description	
Operation	Reboot Shutdown

License Information

Connection Summary

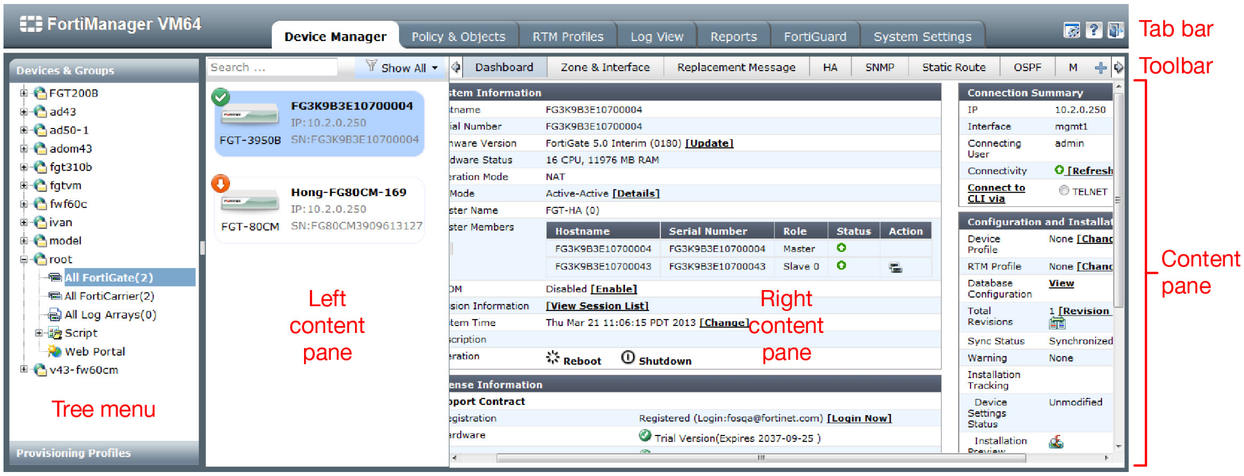
IP	10.2.0.250
Interface	mgmt1
Connecting User	admin
Connectivity	**[Refresh]**
Connect to CLI via	○ TELNET ● SSH

Configuration and Installation Status

Device Profile	None **[Change]**
RTM Profile	None **[Change]**
Database Configuration	**View**
Total Revisions	1 **[Revision History]**
Sync Status	Synchronized **[Refresh]**
Warning	None
Installation Tracking	
Device Settings Status	Unmodified
Installation Preview	
Last Installation	None

When viewing the *Device Manager* tab, you can switch to vertical view by selecting *Preferences* on the navigation pane. In this view, content is displayed vertically in the left content pane and right content pane. For more information, see "Device manager layout" on page 18.

Figure 6: FortiManager Web-based Manager vertical view



stem Information

tname	FG3K9B3E10700004
ial Number	FG3K9B3E10700004
nware Version	FortiGate 5.0 Interim (0180) [Update]
dware Status	16 CPU, 11976 MB RAM
ration Mode	NAT
Mode	Active-Active [Details]
ster Name	FGT-HA (0)
ster Members	

Hostname	Serial Number	Role	Status	Action
FG3K9B3E10700004	FG3K9B3E10700004	Master	✓	
FG3K9B3E10700043	FG3K9B3E10700043	Slave 0	✓	

OM	Disabled [Enable]
sion Information	[View Session List]
tem Time	Thu Mar 21 11:06:15 PDT 2013 [Change]
scription	
ration	Reboot Shutdown

ense Information

pport Contract

egistration	Registered (Login:fosqa@fortinet.com) [Login Now]
rdware	Trial Version(Expires 2037-09-25)

Connection Summary

IP	10.2.0.250
Interface	mgmt1
Connecting User	admin
Connectivity	[Refresh
Connect to CLI via	○ TELNET

Configuration and Installat

Device Profile	None [Chang
RTM Profile	None [Chang
Database Configuration	View
Total Revisions	1 [Revision
Sync Status	Synchronized
Warning	None
Installation Tracking	
Device Settings Status	Unmodified
Installation Preview	

The Web-based Manager includes detailed online help. Selecting *Help* on the Navigation pane opens the online help.

The navigation pane and content pane information displayed to an administrator vary according to the administrator account settings and access profile that have be configured for that user. To configure admin profiles, go to *System Settings* > *Admin* > *Profile*. You can configure the admin profile at both a global and ADOM level with a high degree of granularity in providing read-write, read-only, or restricted access to various Web-based Manager modules. When defining a new administrator, you can further define which ADOMs and policy packages the administrator can access. For more information about administrator accounts and their privileges, see “Admin” on page 78.

When you log in to the FortiManager unit as the `admin` administrator, the Web-based Manager opens to the *Device Manager* tab. You can view all ADOMs in the navigation tree, and ADOM information in the content pane. For more information, see “Device Manager” on page 114.

Configuration changes made using the Web-based Manager take effect immediately without resetting the FortiManager system or interrupting service.

Using the navigation pane

Table 1: Web-based Manager tabs

Tab	Description
Device Manager	Add and manage devices, view the device information and status, create and manage device groups and manage firewall global policy objects. From this menu, you can also configure the web portal configurations, users, and groups. For more information, see "Device Manager" on page 114.
Policy & Objects	Configure policy packages and objects. For more information, see "Policy & Objects" on page 209.
RTM Profiles	Configure RTM profiles that can be applied to your managed devices, allowing for you to easily monitor your devices for trends, outages, or events that require attention. For more information, see "RTM Profiles" on page 228.
Log View	View logs for managed devices. For more information, see "Log View" on page 238.
Reports	Configure report templates, schedules, and output profiles. For more information, see "Reports" on page 252.
FortiGuard	Configure FortiGuard settings, package and query server management, and firmware images. For more information, see "FortiGuard Center" on page 275.
System Settings	Configure system settings such as network interfaces, administrators, system time, server settings, and widgets and tabs. From this menu, you can also perform maintenance and firmware operations. For more details on using this menu, see "System Settings" on page 48.

The navigation pane is dependent on administrator profile settings.

Configuring Web-based Manager settings

Global settings for the Web-based Manager apply regardless of which administrator account you use to log in. Global settings include the idle timeout, TCP port number on which the Web-based Manager listens for connection attempts, the network interface on which it listens, and the display language.

This section includes the following topics:

- Changing the Web-based Manager language
- Administrative access
- Restricting Web-based Manager access by trusted host
- Changing the Web-based Manager idle timeout
- Other security considerations

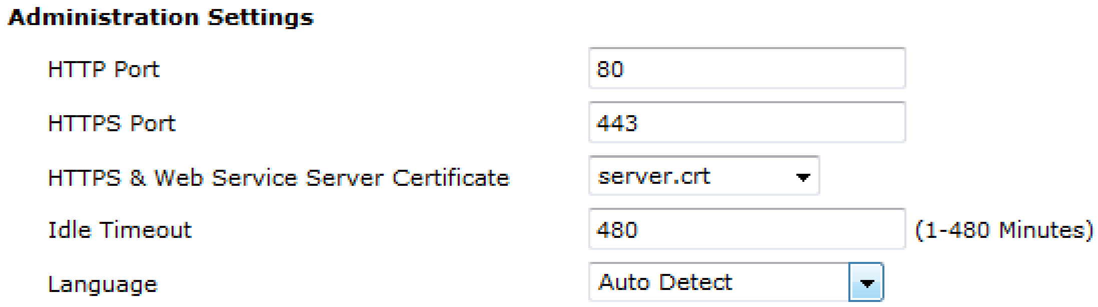
Changing the Web-based Manager language

The Web-based Manager supports multiple languages; the default language is English. You can change the Web-based Manager to display in English, Simplified Chinese, Traditional Chinese, Japanese, or Korean. For best results, you should select the language that the management computer operating system uses. You can also set the FortiManager Web-based Manager to automatically 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* > *Admin* > *Admin Settings*.
2. In the *Language* field, select a language from the drop-down list, or select *Auto Detect* to use the same language as configured for your web browser.
3. Select *OK*.

Figure 7: Administration settings



Administration Settings

HTTP Port	80
HTTPS Port	443
HTTPS & Web Service Server Certificate	server.crt
Idle Timeout	480 (1-480 Minutes)
Language	Auto Detect

Administrative access

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

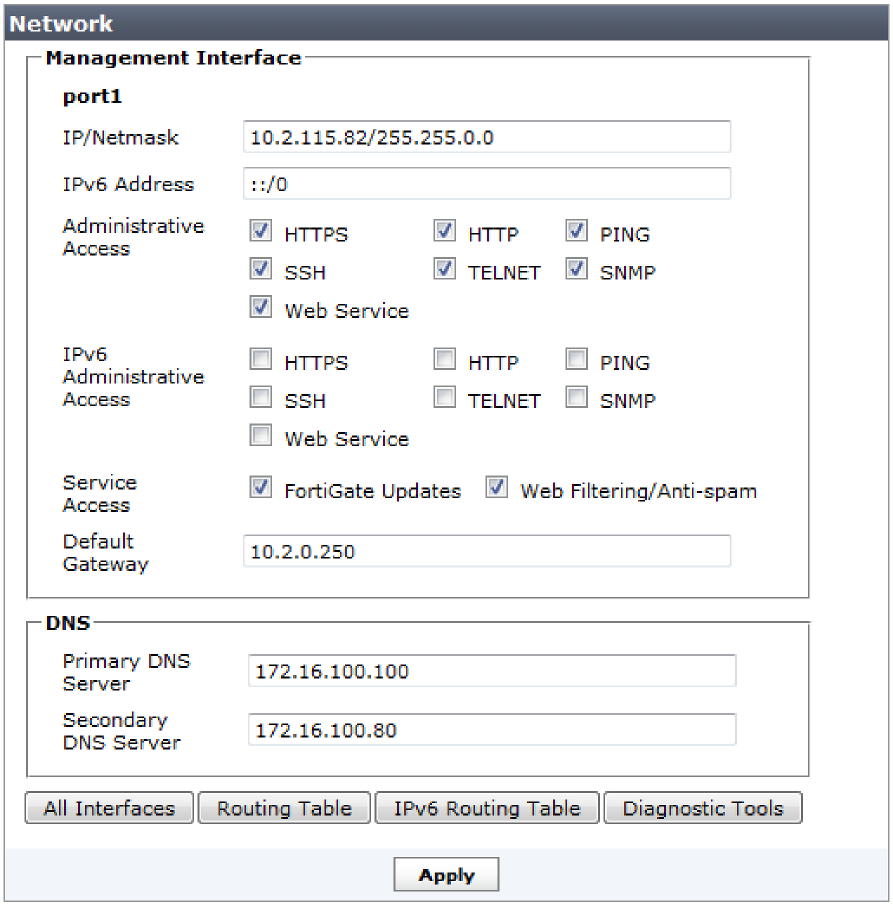
Administrative access can be configured in IPv4 or IPv6 and includes the following settings:

HTTPS	PING	TELNET	Web Service
HTTP	SSH	SNMP	

To change administrative access to your FortiManager system:

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

Figure 8: Management Interface page



Network

Management Interface

port1

IP/Netmask: 10.2.115.82/255.255.0.0

IPv6 Address: ::/0

Administrative Access: ☑ HTTPS ☑ HTTP ☑ PING ☑ SSH ☑ TELNET ☑ SNMP ☑ Web Service

IPv6 Administrative Access: □ HTTPS □ HTTP □ PING □ SSH □ TELNET □ SNMP □ Web Service

Service Access: ☑ FortiGate Updates ☑ Web Filtering/Anti-spam

Default Gateway: 10.2.0.250

DNS

Primary DNS Server: 172.16.100.100

Secondary DNS Server: 172.16.100.80

Administrative access is configured for port1. To configure administrative access for another interface, select *All Interfaces*, and then select the interface to edit.

2. Set the *IPv4 IP/Netmask* or *IPv6 Address*.
3. Select one or more *Administrative Access* types for the interface.
4. Select *Service Access*, *FortiGate Updates*, and *Web Filtering/Antispam* if required.
5. Set the *Default Gateway*.
6. Configure the primary and secondary DNS servers.

7. Select *Apply*.

   In addition to the settings listed above, you can select to enable access on interface from the *All Interfaces* window.

Restricting Web-based Manager access by trusted host

To prevent unauthorized access to the Web-based Manager you can configure administrator accounts with trusted hosts. With trusted hosts configured, the admin user can only log into the Web-based Manager when working on a computer with the trusted host as defined in the admin account. See "Administrator" on page 80 for more details.

Changing the Web-based Manager idle timeout

By default, the Web-based Manager disconnects administrative sessions if no activity takes place for five 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.

To change the Web-based Manager idle timeout:

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

Other security considerations

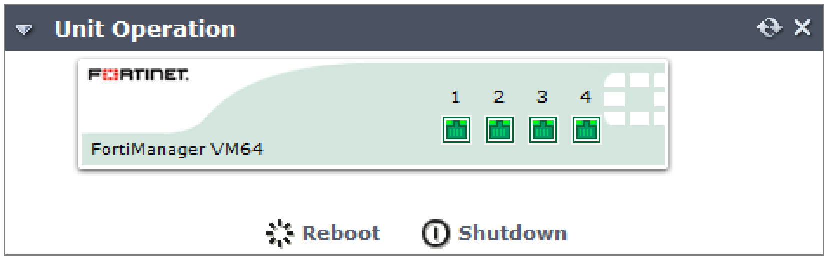
Other security consideration for restricting access to the FortiManager Web-based Manager include the following:

- Configure administrator accounts using a complex passphrase for local accounts
- Configure administrator accounts using RADIUS, LDAP, or TACACS+
- Configure the admin profile to only allow read-write access as required and restrict access using read-only or no access to settings which are not applicable to that administrator
- Configure the administrator account to only allow access to specific ADOMs as required
- Configure the administrator account to only allow access to specific policy packages as required.

Reboot and shutdown of the FortiManager unit

Always reboot and shutdown the FortiManager system using the unit operation options in the Web-based Manager, or using CLI commands, to avoid potential configuration problems.

Figure 9: Unit operation widget



To reboot the FortiManager unit:

1. From the Web-based Manager, go to *System Settings* > *General* > *Dashboard*.
2. In the Unit Operation widget select *Reboot*, or from the CLI Console widget enter:

```
execute reboot
```

To shutdown the FortiManager unit:

1. From the Web-based Manager, go to System *Settings* > *General* > *Dashboard*.
2. In the Unit Operation widget select *Shutdown*, or from the CLI Console widget enter:

```
execute shutdown
```

Administrative Domains

FortiManager appliances scale to manage thousands of Fortinet devices. Administrative domains (ADOMs) enable administrators to manage only those devices that are specific to their geographic location or business division. FortiGate devices with multiple VDOMs can be divided among multiple ADOMs.

If ADOMs are enabled, each administrator account is tied to an ADOM. When a particular administrator logs in, they see only those devices or VDOMs that have been enabled for their account. Administrator accounts that have special permissions, such as the `admin` account, can see and maintain all ADOMs and the devices within those domains.

ADOMs are not enabled by default, and enabling and configuring the domains can only be performed by the `admin` administrator. For more information, see “Enabling and disabling the ADOM feature” on page 41.

The default and maximum number of ADOMs you can add depends on the FortiManager system model and the available ADOM license key. Please refer to the FortiManager datasheet for information on the maximum number of devices that your model supports. You can contact your local Fortinet reseller to purchase an ADOM licence to increase the number of device ADOMs.

This section includes the following topics:

- Enabling and disabling the ADOM feature
- About ADOM modes
- Managing ADOMs

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

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

- Firmware version: group all devices with the same firmware version into an ADOM.
- Geographic regions: group all devices for a specific geographic region into an ADOM, and devices for a different region into another ADOM.
- Administrative users: group devices into separate ADOMs based for specific administrators responsible for the group of devices.
- Customers: group all devices for one customer into an ADOM, and devices for another customer into another ADOM.
- Device type: create a separate ADOM for each device type.

Enabling and disabling the ADOM feature

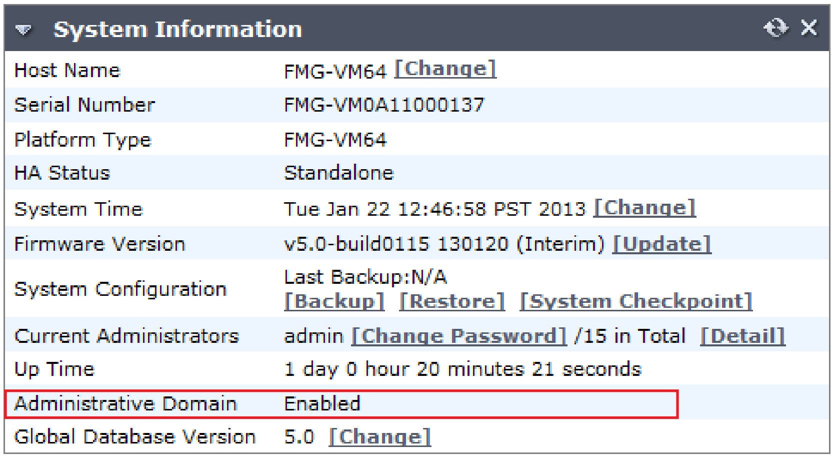
To enable or disable the ADOM feature, you must be logged in as the `admin` administrator. Only this user has the ability to enable or disable this feature.

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

To enable the ADOM feature

1. Log in as `admin`.
2. Go to *System Settings* > *General* > *Dashboard.*
3. In the system information widget, select *Enable* next to *Administrative Domain*

Figure 10: Enabling ADOMs



System Information

Host Name	FMG-VM64 [Change]
Serial Number	FMG-VM0A11000137
Platform Type	FMG-VM64
HA Status	Standalone
System Time	Tue Jan 22 12:46:58 PST 2013 [Change]
Firmware Version	v5.0-build0115 130120 (Interim) [Update]
System Configuration	Last Backup:N/A [Backup] [Restore] [System Checkpoint]
Current Administrators	admin [Change Password] /15 in Total [Detail]
Up Time	1 day 0 hour 20 minutes 21 seconds
Administrative Domain	Enabled
Global Database Version	5.0 [Change]

To disable the ADOM feature

1. Remove all the managed devices from all ADOMs.
2. Delete all non-root ADOMs, by right-clicking on the ADOM in the tree menu in the *Device Manager* tab and selecting *Delete* from the pop-up menu.

   After removing the ADOMs, you can now disable the ADOM feature.
3. Go to *System Settings* > *General* > *Dashboard.*
4. In the system information widget, select *Disable* next to *Administrative Domain.*

About ADOM modes

When the ADOMs feature is enabled and you log in as the `admin` user, all the available ADOMs will be listed in the tree menus on different tabs.

In the *Policy & Objects* tab, a menu bar is available that allows to select either *Global*, or a specific ADOM from the drop-down list. Selecting *Global* or a specific ADOM will then display the policy packages and objects appropriate for your selection.

Switching between ADOMs

As an `admin` administrator, you are able to move between all the ADOMs created on the FortiManager system. This enables you to view, configure and manage the various domains.

Other administrators are only able to move between the ADOMs to which they have been given access. They are able to view and administer the domains based on their account‘s permission settings.

To access a specific ADOM, simply select that ADOM in the tree menu. The FortiManager system presents you with the available options for that domain, depending on what tab you are currently using.

Normal mode ADOMs

When creating an ADOM in *Normal Mode*, the ADOM is considered *Read/Write*, where you are able to make changes to the ADOM and managed devices from the FortiManager. FortiGate units in the ADOM will query their own configuration every 5 seconds. If there has been a configuration change, the FortiGate unit will send a diff revision on the change to the FortiManager using the FGFM protocol.

Backup mode ADOMs

When creating an ADOM in Backup Mode, the ADOM is consider *Read Only*, where you are not able to make changes to the ADOM and managed devices from the FortiManager. Changes are made via scripts which are run on the managed device, or through the device's Web-based Manager or CLI directly. Revisions are sent to the FortiManager when specific conditions are met:

- Configuration change and session timeout
- Configuration change and logout
- Configuration change and reboot
- Manual configuration backup from the managed device.

Backup mode enables you to configure an ADOM where all the devices that are added to the ADOM will only have their configuration backed up. Configuration changes cannot be made to the devices in backup ADOM. You can push any existing revisions to managed devices. You can still monitor and review the revision history for these devices, and scripting is still allowed for pushing scripts directly to FortiGate units.

Managing ADOMs

When the ADOMs feature is enabled and you log in as the `admin` user, all the available ADOMs will be listed in the tree menus on the different available tabs. In the *Policy & Objects* tab, a menu bar is available that allows to select either *Global*, or a specific ADOM from the drop-down list. Selecting *Global* or a specific ADOM will then display the policy packages and objects appropriate for your selection.

To configure and manage ADOMs, go to the *Device Manager* tab, or to *System Settings > General > All ADOMs*. See "All ADOMS" on page 68 for more information.

Extend workspace to entire ADOM

When concurrent ADOM access is enabled, administrators are able to lock the ADOM. A right-click menu option has been added to allow you to lock/unlock ADOM access. The ADOM lock status is displayed by a lock icon to the left of the ADOM name. The lock status is as follows:

- Grey lock: The ADOM is currently unlocked, and is read/write.
- Green lock: The ADOM is locked by you when logged in as an admin.
- Red lock: The ADOM is locked by another admin.

An additional CLI command has been added to enable or disable ADOM lock override:

```
config system global
  set lock-preempt [enable | disable]
end
```

When the ADOM lock override is enabled, if two administrators are concurrently accessing an ADOM and one attempts to lock the ADOM, the other admin can kick the admin off the ADOM, preventing the ADOM from being locked.

Workspace is disabled by default, and is enabled on the CLI console. When workspace is enabled, the Device Manager and Policy & Objects tabs are read-only. You must lock the ADOM to enable read-write access to make changes to the ADOM.

Concurrent ADOM access

System administrators can enable or disable concurrent access to the same ADOM if multiple administrators are responsible for managing a single ADOM. When enabled, multiple administrators can log in to the same ADOM concurrently. When disabled, only a single administrator has read/write access to the ADOM, while all other administrators have read-only access.

Concurrent ADOM access can be enabled or disabled using the CLI.

Concurrent ADOM access is enabled by default. To prevent concurrent administrators from making changes to the FortiManager database at the same time, and thereby causing conflicts, you must enable the workspace function.

To enable ADOM locking and disable concurrent ADOM access:

```
config system global
  set workspace enable
end
```

To disable ADOM locking and enable concurrent ADOM access:

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

Adding an ADOM

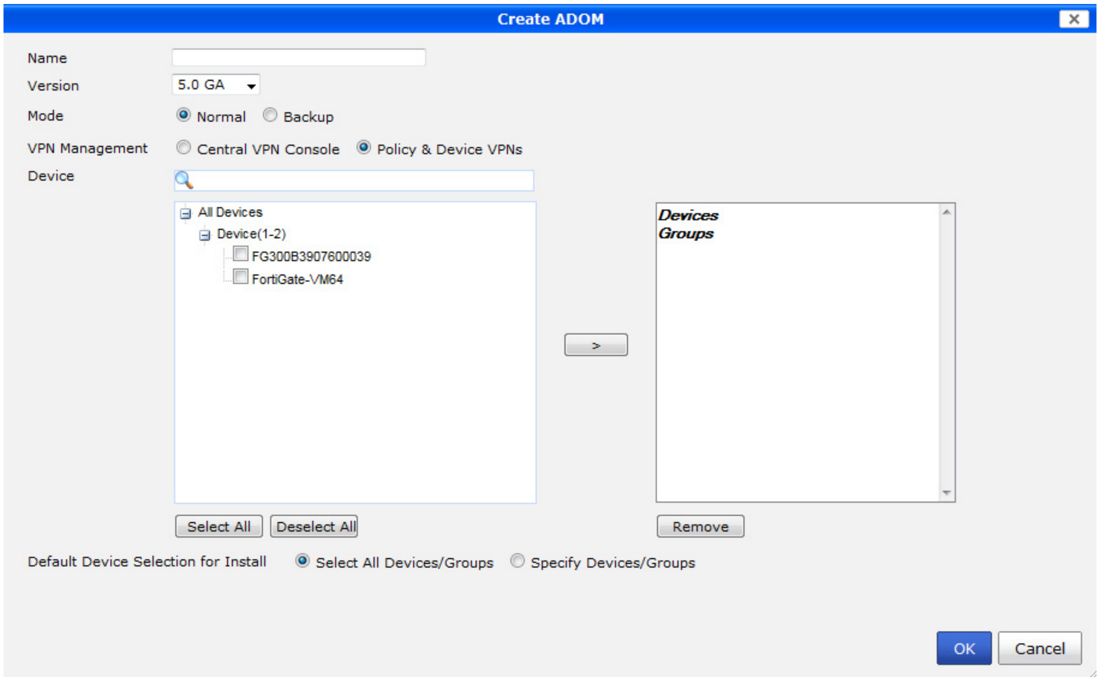
To add an ADOM, you must be logged in as the `admin` administrator. You must also first enable administrative domains in the Web-based Manager; see “To enable the ADOM feature” on page 42.

To create an ADOM

1. Do one of the following:
    - Go to the *Device Manager* tab and right-click on an ADOM name in the tree menu and, under the *ADOM* heading in the pop-up menu, select *Create New*.
    - Go to *System Settings* > *General* > *All ADOMs* and either select *Create New*, or right-click in the content pane and select *New* from the pop-up menu.

    The *Create ADOM* dialog box will open which will allow you to configure the new ADOM.

Figure 11: Create ADOM dialog box



Create ADOM

Name

Version 5.0 GA

Mode ● Normal ○ Backup

VPN Management ○ Central VPN Console ● Policy & Device VPNs

Device

- All Devices
  - Device(1-2)
    - □ FG300B3907600039
    - □ FortiGate-VM64

Default Device Selection for Install ● Select All Devices/Groups ○ Specify Devices/Groups

2. Enter the following information:

Name	Enter a name that will allow you to distinguish this ADOM from your other ADOMs.
Version	Select the version of FortiGate devices in the ADOM. FortiManager v5.0 supports FortiOS v5.0, v4.0 MR3, and v4.0 MR2.
Mode	Select *Normal* mode if you want to manage and configure the connected FortiGate devices from the FortiManager Web-based Manager. Select *Backup* mode if you want to backup the FortiGate configurations to the FortiManager, but configure each FortiGate locally.
VPN Management	Select *Central VPN Console* or select *Policy & Device VPNs*.
Device	Select members from the *Available member* list and transfer them to the *Selected member* list to assign the devices to the ADOM.
Default Device Selection for Install	Select either *Select All Devices/Groups* or *Specifiy Devices/Groups*.

3. Select *OK* to create the ADOM.

Deleting an ADOM

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

To delete an ADOM

1. In the *Device Manager* tab, right-click on an ADOM name in the tree menu and, under the *ADOM* heading in the pop-up menu, select *Delete*.

The root ADOM cannot be deleted.

2. In the confirmation dialog box, select *OK*.

Assigning devices to an ADOM

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

To assign devices to an ADOM

1. In the *Device Manager* tab, right-click on the ADOM to which you want to assign a device in the tree menu and, under the *ADOM* heading in the pop-up menu, select *Edit*.

   The *Edit ADOM* dialog box will open.
2. From the *Available member* list, select which devices you want to associate with the ADOM and select the right arrow to move them to the *Selected member* list.

   If the administrative device mode is *Advanced*, you can add separate FortiGate VDOMs to the ADOM as well as FortiGate units. For more information see "ADOM device modes" on page 46.
3. When done, select *OK*. The selected devices appear in the device list for that ADOM.

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.

ADOM device modes

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

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

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

```
config system 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 ADOM.

Assigning administrators to an ADOM

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

By default, when ADOMs are enabled, existing administrator accounts other than `admin` are assigned to the `root` domain, which contains all devices in the device list. For more information about creating other ADOMs, see "Assigning devices to an ADOM" on page 46.

To assign an administrator to an ADOM

1. Log in as `admin`.

   Other administrators cannot configure administrator accounts when ADOMs are enabled.
2. Go to *System Settings* > *Admin* > *Administrator*.
3. Configure the administrator account, and select the *Admin Domains* that the administrator account will be able to use to access the FortiManager system.

Do not select *Edit* for the `admin` account. The `admin` administrator account cannot be restricted to an ADOM.

System Settings

The System Settings tab enables you 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 Update Service* for updates.

Additional configuration options and short-cuts are available using the right-click menu. Right-click the mouse on different navigation panes on the Web-based Manager page to access these options.

The *System Settings* tab provides access to the following menus and sub-menus:

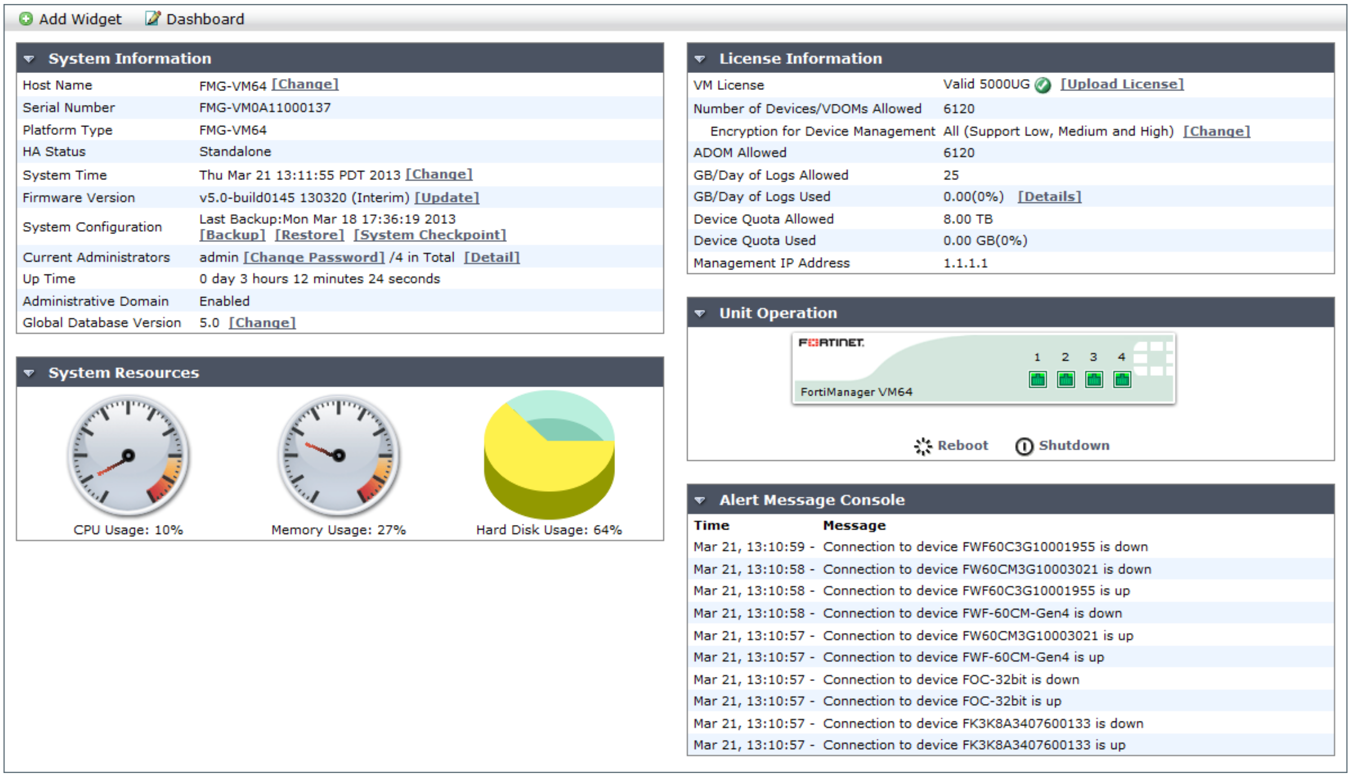
General	Select this menu to configure, monitor, and troubleshoot the main system information. • Dashboard • All ADOMS • Network • Certificates • High Availability • Log access • Diagnostic tools
Admin	Select this menu to configure administrator user accounts, as well as configure global administrative settings for the FortiManager unit. • Monitoring administrator sessions • Administrator • Profile • Remote authentication server • Administrator settings
FortiGuard Center	See "FortiGuard Center" on page 275 for information.
Advanced	Select to configure mail server settings, remote output, SNMP, meta field data and other advanced settings. • SNMP v1/v2c • Meta fields • Advanced settings • Alerts • Device Log

Dashboard

When you select the *System Settings* tab, it automatically opens at the *System Settings* > *General* > *Dashboard* page; see Figure 12.

The Dashboard page displays widgets that provide performance and status information and enable you to configure basic system settings. The dashboard also contains a CLI widget that enables you to use the command line through the Web-based Manager. These widgets appear on a single dashboard.

Figure 12: FortiManager system dashboard



System Information

Host Name	FMG-VM64 [Change]
Serial Number	FMG-VM0A11000137
Platform Type	FMG-VM64
HA Status	Standalone
System Time	Thu Mar 21 13:11:55 PDT 2013 [Change]
Firmware Version	v5.0-build0145 130320 (Interim) [Update]
System Configuration	Last Backup:Mon Mar 18 17:36:19 2013 [Backup] [Restore] [System Checkpoint]
Current Administrators	admin [Change Password] /4 in Total [Detail]
Up Time	0 day 3 hours 12 minutes 24 seconds
Administrative Domain	Enabled
Global Database Version	5.0 [Change]

System Resources

CPU Usage: 10%

Memory Usage: 27%

Hard Disk Usage: 64%

License Information

VM License	Valid 5000UG ✓ [Upload License]
Number of Devices/VDOMs Allowed	6120
Encryption for Device Management	All (Support Low, Medium and High) [Change]
ADOM Allowed	6120
GB/Day of Logs Allowed	25
GB/Day of Logs Used	0.00(0%) [Details]
Device Quota Allowed	8.00 TB
Device Quota Used	0.00 GB(0%)
Management IP Address	1.1.1.1

Unit Operation

Alert Message Console

```
Time                Message
Mar 21, 13:10:59 -  Connection to device FWF60C3G10001955 is down
Mar 21, 13:10:58 -  Connection to device FW60CM3G10003021 is down
Mar 21, 13:10:58 -  Connection to device FWF60C3G10001955 is up
Mar 21, 13:10:58 -  Connection to device FWF-60CM-Gen4 is down
Mar 21, 13:10:57 -  Connection to device FW60CM3G10003021 is up
Mar 21, 13:10:57 -  Connection to device FWF-60CM-Gen4 is up
Mar 21, 13:10:57 -  Connection to device FOC-32bit is down
Mar 21, 13:10:57 -  Connection to device FOC-32bit is up
Mar 21, 13:10:57 -  Connection to device FK3K8A3407600133 is down
Mar 21, 13:10:57 -  Connection to device FK3K8A3407600133 is up
```

The following widgets are available:

System Information

Displays basic information about the FortiManager system, such as up time and firmware version. For more information, see “General settings” on page 68.

From this widget you can also manually update the FortiManager firmware to a different release. For more information, see “Firmware images” on page 295.

License Information

Displays the devices being managed by the FortiManager unit and the maximum numbers of devices allowed. For more information, see “License Information widget” on page 61.

Unit Operation

Displays status and connection information for the ports of the FortiManager unit. It also enables you to shutdown and restart the FortiManager unit or reformat a hard disk. For more information, see “Unit Operation widget” on page 62.

System Resources	Displays the real-time and historical usage status of the CPU, memory and hard disk. For more information, see "System Resource widget" on page 59.
Alert Message Console	Displays log-based alert messages for both the Fortinet unit itself and connected devices. For more information, see "Alert Messages Console widget" on page 63.
CLI Console	Opens a terminal window that enables you to configure the FortiManager unit using CLI commands directly from the Web-based Manager. This widget is hidden by default. For more information, see "CLI Console widget" on page 64.
RAID Monitor	Displays information about the status of RAID disks as well as what RAID level has been selected. It also displays how much disk space is currently consumed. For more information, see "RAID Monitor widget" on page 64.

Customizing the dashboard

The FortiManager system dashboard can be customized. You can select which widgets to display, where they are located on the page, and whether they are minimized or maximized.

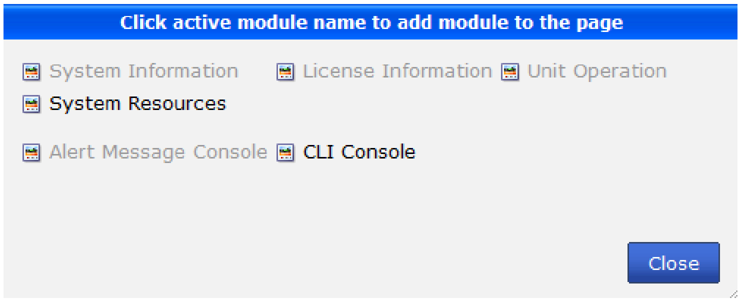
To move a widget

Position your mouse cursor on the widget's title bar, then click and drag the widget to its new location.

To add a widget

In the dashboard toolbar, select *Add Widget*, then select the names of widgets that you want to show. To hide a widget, in its title bar, select the *Close* icon.

Figure 13: Adding a widget


Click active module name to add module to the page

System Information
License Information
Unit Operation
System Resources
Alert Message Console
CLI Console

Multiple *System Resources* widgets can be added to the dashboard. Only one of all of the other widgets may be added.

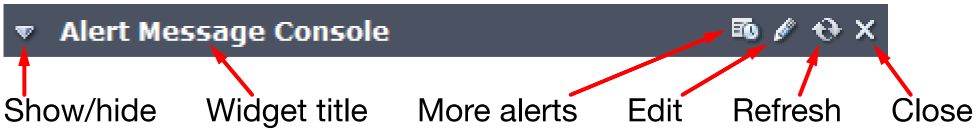
To reset the dashboard

Select *Dashboard* > *Reset Dashboard* from the dashboard toolbar.

To see the available options for a widget

Position your mouse cursor over the icons in the widget's title bar. Options vary slightly from widget to widget, but always include options to close or show/hide the widget.

Figure 14:A minimized widget

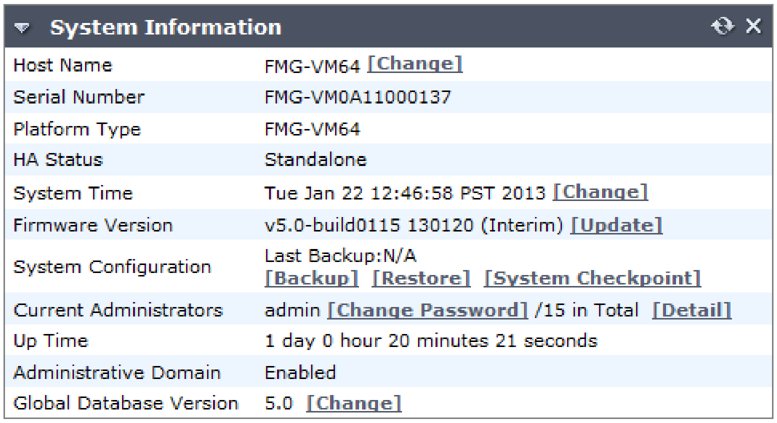


Show/Hide arrow	Display or minimize the widget.
Widget Title	The name of the widget.
More Alerts	Show the *Alert Messages* dialog box. This option appears only on the Alert Message Console widget.
Edit	Select to change settings for the widget. This option appears only on certain widgets.
Detach	Detach the CLI Console widget from the dashboard and open it in a separate window. This option appears only on the CLI Console widget.
RAID Settings	Show the *RAID Settings* dialog box, which displays the current RAID settings and allows for configuration of the RAID level if available. This option appears only on the RAID Monitor widget.
Refresh	Select to update the displayed information.
Close	Select to remove the widget from the dashboard. You will be prompted to confirm the action. To add the widget, select *Widget* in the toolbar and then select the name of the widget you want to show.

System Information widget

The system dashboard includes a System Information widget, shown in Figure 15, which displays the current status of the FortiManager unit and enables you to configure basic system settings.

Figure 15: System Information widget



System Information

Host Name	FMG-VM64 [Change]
Serial Number	FMG-VM0A11000137
Platform Type	FMG-VM64
HA Status	Standalone
System Time	Tue Jan 22 12:46:58 PST 2013 [Change]
Firmware Version	v5.0-build0115 130120 (Interim) [Update]
System Configuration	Last Backup:N/A [Backup] [Restore] [System Checkpoint]
Current Administrators	admin [Change Password] /15 in Total [Detail]
Up Time	1 day 0 hour 20 minutes 21 seconds
Administrative Domain	Enabled
Global Database Version	5.0 [Change]

The following information is available on this widget:

Host Name	The identifying name assigned to this FortiManager unit. For more information, see “Changing the host name” on page 53.
Serial Number	The serial number of the FortiManager unit. The serial number is unique to the FortiManager unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
Platform Type	Displays the FortiManager platform type, for example *FMG-VM* (virtual machine).
HA Status	Displays if FortiManager unit is in High Availability mode and whether it is the Master or Slave unit in the HA cluster. For more information see “High Availability” on page 297.
System Time	The current time on the FortiManager internal clock. For more information, see “Configuring the system time” on page 54.
Firmware Version	The version number and build number of the firmware installed on the FortiManager unit. To update the firmware, you must download the latest version from the Customer Service & Support web site at https://support.fortinet.com. Select *Update* and select the firmware image to load from the local hard disk or network volume. For more information, see “Updating the system firmware” on page 55.

System Configuration	The date of the last system configuration backup. The following actions are available: • Select *Backup* to backup the system configuration to a file; see "Backing up the system" on page 56. • Select *Restore* to restore the configuration from a backup file; see "Restoring the configuration" on page 57. • Select *System Checkpoint* to revert the system to a prior saved configuration; see "Creating a system checkpoint" on page 58.
Current Administrators	The number of administrators that are currently logged in. The following actions are available: • Select *Change Password* to change your own password. • Select *Details* to view the session details for all currently logged in administrators. See "Monitoring administrator sessions" on page 79 for more information.
Up Time	The duration of time the FortiManager unit has been running since it was last started or restarted.
Administrative Domain	Displays whether ADOMs are enabled.
Global Database Version	Displays the current Global Database version.

Changing the host name

The host name of the Fortinet unit is used in several places.

- It appears in the *System Information* widget on the *Dashboard*. For more information about the *System Information* widget, see "System Information widget" on page 52.
- It is used in the command prompt of the CLI.
- It is used as the SNMP system name. For information about SNMP, see "SNMP v1/v2c" on page 93.

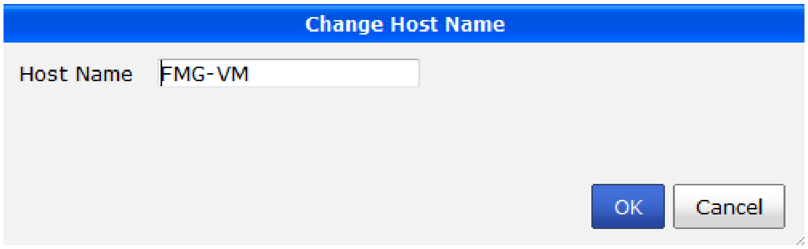
The System Information widget and the `get system status` CLI command will display the full host name. However, if the host name is longer than 16 characters, the CLI and other places display the host name in a truncated form ending with a tilde (~) to indicate that additional characters exist, but are not displayed. For example, if the host name is Fortinet1234567890, the CLI prompt would be `Fortinet123456~#`.

To change the host name

1. Go to *System Settings > General > Dashboard*.
2. In the *System Information* widget, next to the *Host Name* field, select *Change*.

   The *Change Host Name* dialog box opens.

   Figure 16: Edit Host Name dialog box

   Host Name: FMG-VM

3. In the *Host Name* field, type a new host name.

   The host name may be up to 35 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.

4. Select *OK*.

Configuring the system time

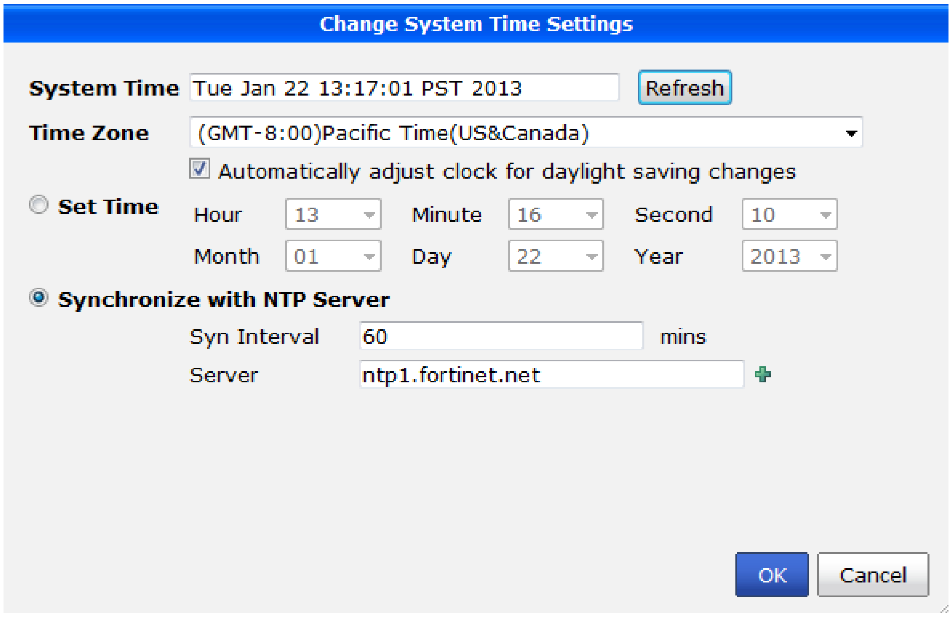
You can either manually set the Fortinet system time or configure the Fortinet unit to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.

For many features to work, including scheduling, logging, and SSL-dependent features, the Fortinet system time must be accurate.

To configure the date and time

1. Go to *System Settings* > *General* > *Dashboard*.
2. In the *System Information* widget, in the *System Time* field, select *Change*. The *Change System Time Settings* dialog box appears, see Figure 17.

Figure 17: Time Settings dialog box



Change System Time Settings

System Time: Tue Jan 22 13:17:01 PST 2013 [Refresh]

Time Zone: (GMT-8:00)Pacific Time(US&Canada)

☑ Automatically adjust clock for daylight saving changes

○ Set Time
Hour 13 Minute 16 Second 10
Month 01 Day 22 Year 2013

● Synchronize with NTP Server
Syn Interval: 60 mins
Server: ntp1.fortinet.net

[OK] [Cancel]

3. Configure the following settings to either manually configure the system time, or to automatically synchronize the Fortinet unit’s clock with an NTP server:

System Time	The date and time according to the Fortinet unit’s clock at the time that this tab was loaded, or when you last selected the *Refresh* button.
Time Zone	Select the time zone in which the Fortinet unit is located and whether or not the system automatically adjusts for daylight savings time.

Set Time	Select this option to manually set the date and time of the Fortinet unit's clock, then select the *Hour*, *Minute*, *Second*, *Year*, *Month*, and *Day* fields before you select *OK*.
Synchronize with NTP Server	Select this option to automatically synchronize the date and time of the Fortinet unit's clock with an NTP server, then configure the *Syn Interval* and *Server* fields before you select *OK*.
Sync Interval	Enter how often in minutes the Fortinet unit should synchronize its time with the NTP server. For example, entering 1440 causes the Fortinet unit to synchronize its time once a day.
Server	Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, go to http://www.ntp.org.

4. Select *OK* to apply your changes.

Updating the system firmware

To take advantage of the latest features and fixes, FortiManager provides two ways to upgrade its firmware: manually or through the FDN.

Back up the configuration and database before changing the firmware of your Fortinet unit. Changing the firmware to an older or incompatible version may reset the configuration and database to the default values for that firmware version, resulting in data loss. For information on backing up the configuration, see "Backing up the system" on page 56.

Before you can download firmware updates for your Fortinet unit, you must first register your Fortinet unit with Customer Service & Support. For details, go to https://support.fortinet.com/ or contact Customer Service & Support.

To manually update the Fortinet firmware

1. Download the firmware (the `.out` file) from the Customer Service & Support web site, https://support.fortinet.com/.
2. Go to *System Settings* > *General* > *Dashboard*.
3. In the *System Information* widget, in the *Firmware Version* field, select *Update*. The Firmware Upgrade window opens.
4. Select *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support web site, and select *Open*.
5. Select *OK* to upload the file.

   Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, a prompt appears:

   "`Manual upload release complete. It will take a few minutes to unpack the uploaded release. Please wait.`"
6. Wait until the unpacking process completes, then refresh the page. The firmware package file name will appear in the *Releases Available For Upgrade* section after you refresh the page.

7. Select the firmware package, then select the icon in the *Upgrade Firmware* column and select *OK* in the dialog box that appears. The Fortinet unit installs the firmware and restarts.

   If you changed the firmware to an earlier version whose configuration is not compatible, you may need to do first-time setup again. For instructions, see the *FortiManager QuickStart Guide* for your unit.

8. Update the vulnerability management engine and definitions. For details, see "FortiGuard Center" on page 275.

Installing firmware replaces the current network vulnerability management engine with the version included with the firmware release that you are installing. After you install the new firmware, make sure that your vulnerability definitions are up-to-date. For more information, see "FortiGuard Center" on page 275.

To change the FortiManager system firmware through FDN

1. The FortiManager system can automatically download firmware updates from FDN if you have a valid support license. To access these updates, go to *System Settings > General > Dashboard*.
2. In the *System Information* widget, in the *Firmware Version* row, select *Update*.

   The *Firmware Upgrade* dialog box appears.

   When new versions of firmware are available on FDN, new entries are shown in the *From Server* drop-down list.
3. Select the *Download* icon to start downloading the new upgrade firmware. The time required varies by the size of the file and the speed of your network connection.
4. Wait until the unpacking process completes, then refresh the page. The new firmware package will appear in the *Releases Available For Upgrade* section after you refresh the page.
5. Select the firmware package, then select the icon in the *Upgrade Firmware* column and select *OK* in the dialog box that appears. The Fortinet unit installs the firmware and restarts.

Upgrading firmware through FDN requires proper setup.

FortiManager does not support downgrading firmware to an older version.

Backing up the system

Fortinet recommends that you back up your FortiManager configuration to your management PC or central management server on a regular basis to ensure that, should the system fail, you can quickly get the system back to its original state with minimal affect to the network. You should also perform a back up after making any changes to the FortiManager configuration or settings that affect the managed devices.

You can perform backups manually or at scheduled intervals. You can also create a backups - called checkpoints - that define a point where the FortiManager and network management is stable and functioning. Should any future configurations cause issues, you have a point where the system is stable.

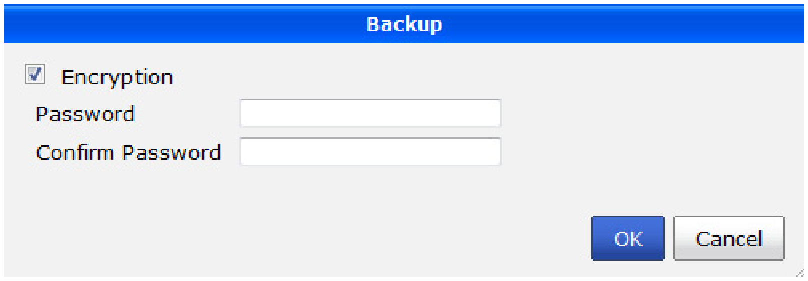
Fortinet recommends backing up all configuration settings from your FortiManager unit before upgrading the FortiManager firmware.

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 > Dashboard*.
2. In the System Information widget, under *System Configuration*, select *Backup*. The *Backup* dialog box opens.

Figure 18: Backup dialog box



Backup

☑ Encryption

Password

Confirm Password

3. Configure the following settings:

Encryption	Select to encrypt the backup file with a password. The password is required to restore the configuration. The check box is selected by default.
Password	(Optional) Select a password. This password is used to encrypt the backup file, and is required to restore the file. (This option is available only when the encryption check box is selected.)
Confirm Password	Re-enter the password to confirm it.

4. If you want to encrypt the backup file, select the *Encryption* check box, then enter and confirm the password you want to use.
5. Select *OK* and save the backup file on your management computer.

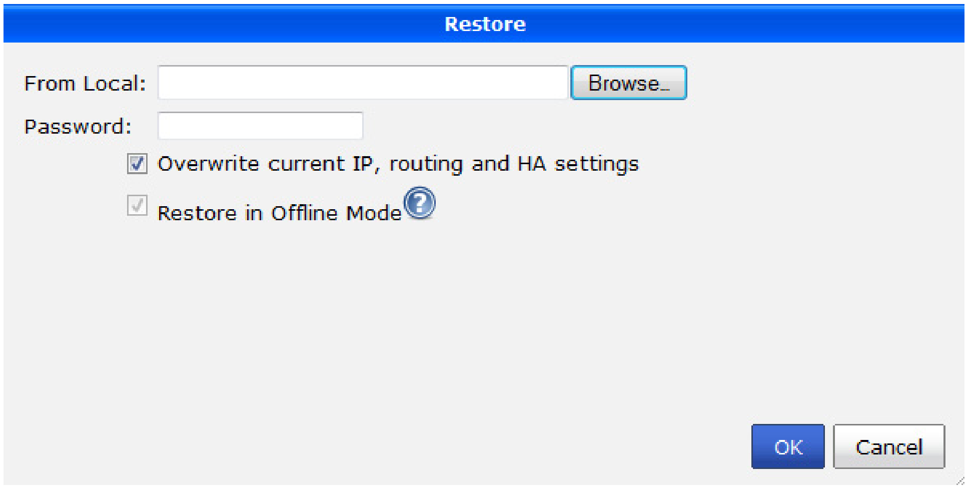
Restoring the configuration

You can use the following procedure to restore your FortiManager configuration from a backup file on your management computer. If your FortiManager unit is in HA mode, switch to Standalone mode.

To restore the FortiManager configuration:

1. Go to *System Settings > General > Dashboard*.
2. In the System Information widget, under *System Configuration*, select *Restore*. The *Restore* dialog box appears; see Figure 19.

Figure 19: All Settings Configuration Restore dialog box


Restore
From Local:
Browse...
Password:
☑ Overwrite current IP, routing and HA settings
☑ Restore in Offline Mode
OK
Cancel

3. Configure the following settings and select OK.

From Local	Select *Browse* to find the configuration backup file you want to restore.
Password	Enter the encryption password, if applicable.
Overwrite current IP, routing and HA settings	Select the check box to overwrite the current IP, routing and HA settings.
Restore in Offline Mode	Informational check box. Hover over help icon for more information.

Creating a system checkpoint

You can create a system checkpoint backup to capture a specific configuration. This backup provides a history where the FortiManager and FortiGate units are completely in sync. Should there be a major failure, you can completely revert the 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.

You should make a system checkpoint backup before installing new firmware to devices or making a major configuration change to the network. If the update or modification causes problems, you can quickly revert to an earlier known “good” version of the configuration to restore operation.

A system checkpoint backup includes:

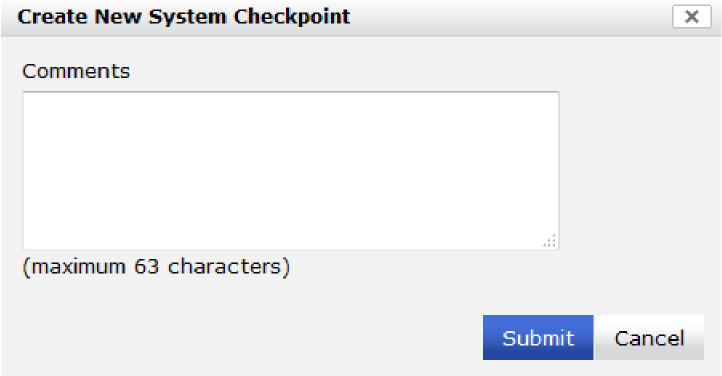
- the current configuration file from each managed device
- the entire system configuration of the FortiManager unit.

To create a checkpoint backup:

1. Go to *System Settings* > *General* > *Dashboard*.
2. In the System Information widget, under *System Configuration*, select *System Checkpoint*.
3. Select *Create New*.

   The Create New System Checkpoint dialog box opens.

Figure 20: Create new system checkpoint



Create New System Checkpoint

Comments

(maximum 63 characters)

4. In the *Comments* field, enter a description, up to 63 characters, for the reason or state of the backup.
5. Select *Submit*.

System Resource widget

The System Resources widget on the dashboard displays the usage status of the CPU, memory and hard disk. You can view system resource information in both real-time and historical format.

Figure 21: System Resource widget (Real Time display)

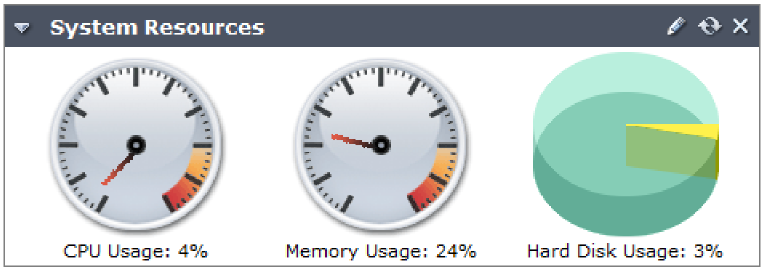
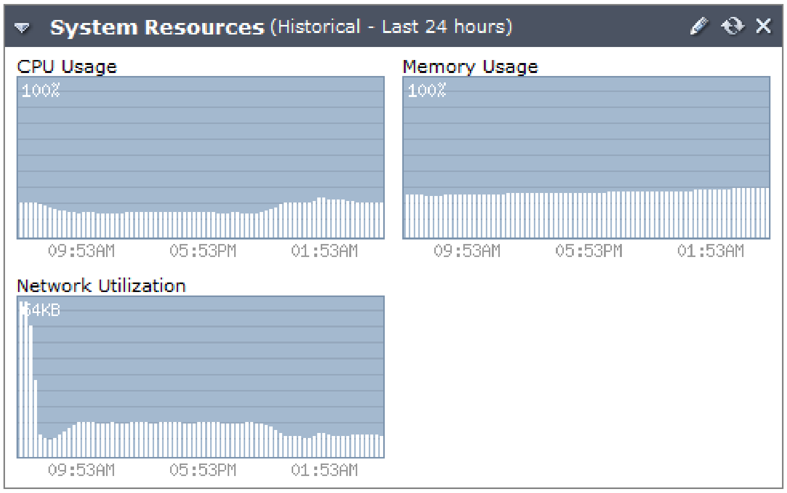


Figure 22: System Resource widget (Historical display)



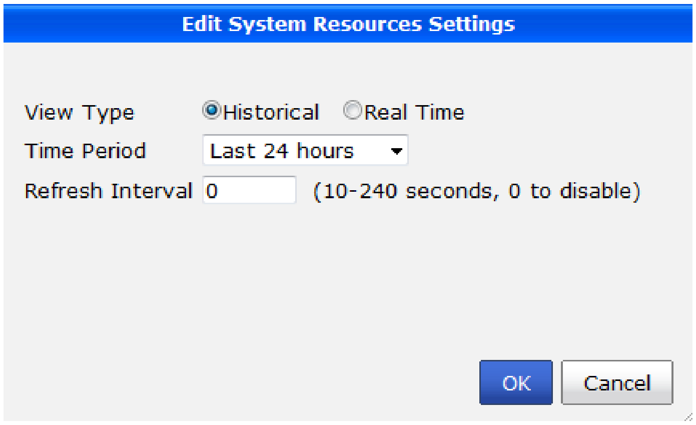
CPU Usage	The current CPU utilization. The Web-based Manager displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the Web-based Manager) is excluded.
Memory Usage	The current memory utilization. The Web-based Manager displays memory usage 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 usage, shown on a pie chart as a percentage of total hard disk space. This item does not appear when viewing historical system resources.
Network Utilization	The network utilization over the specified historical time period. This item does not appear when viewing current (Real Time) system resources.

Change the system resource widget display settings:

1. Go to *System Settings* > *General* > *Dashboard*.
2. In the System Resources widget, hover the mouse over the title bar and select the *Edit* icon.

   The *Edit System Resources Settings* dialog box appears.

Figure 23: Edit System Resources Settings window



Edit System Resources Settings

View Type ● Historical ○ Real Time

Time Period Last 24 hours

Refresh Interval 0 (10-240 seconds, 0 to disable)

3. You can configure the following settings:
    - To view only the most current information about system resources, from *View Type*, select *Real Time*. This is the default.
    - To view historical information about system resources, from *View Type*, select *History*. To change the time range, from *Time Period*, select one of the following: *Last 10 minutes*, *Last 1 hour,* or *Last 24 hours*.
    - To automatically refresh the widget at intervals, in *Refresh Interval*, type a number between 10 and 240 seconds. To disable the refresh interval feature, type `0`.
4. Select *OK* to apply your settings.

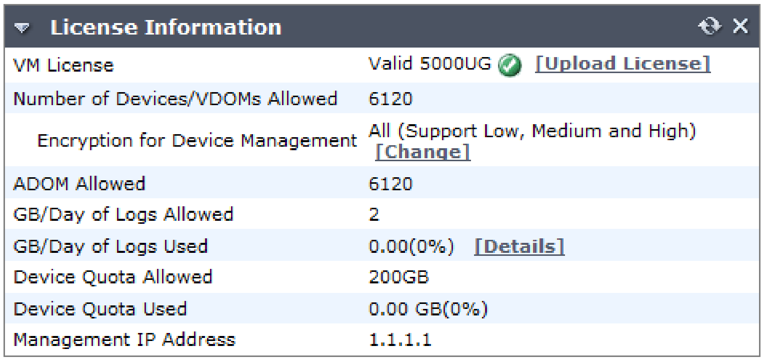
License Information widget

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 intrusion protection signatures or provide web filter and email filter services either from FortiGuard services directly or from the FortiManager updates.

The options available within the License Information widget will vary as different models may not support the same functions. See the FortiManager Family datasheet for more information on your specific device.

Figure 24:VM License Information widget



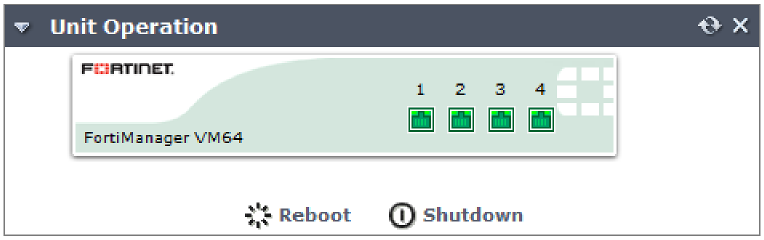
License Information

VM License	Valid 5000UG [Upload License]
Number of Devices/VDOMs Allowed	6120
Encryption for Device Management	All (Support Low, Medium and High) [Change]
ADOM Allowed	6120
GB/Day of Logs Allowed	2
GB/Day of Logs Used	0.00(0%) [Details]
Device Quota Allowed	200GB
Device Quota Used	0.00 GB(0%)
Management IP Address	1.1.1.1

Unit Operation widget

The Unit Operation widget on the dashboard is a graphical representation of the FortiManager unit. It displays status and connection information for the ports on the FortiManager unit. It also enables you to reboot or shutdown the FortiManager hard disk with a quick click of the mouse.

Figure 25: Unit Operation widget



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.
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.

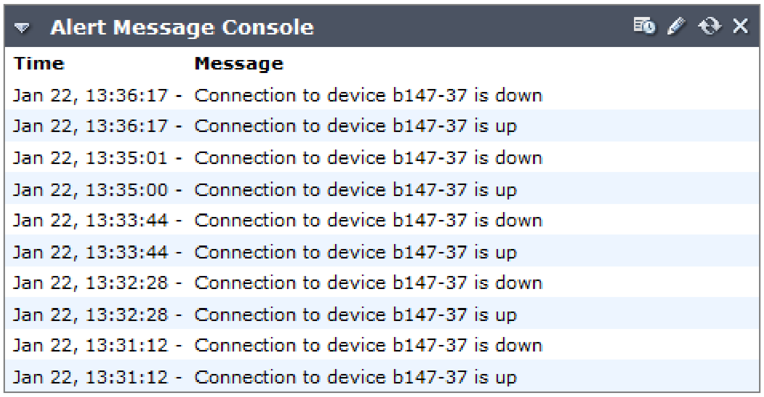
Alert Messages Console widget

The Alert Message Console widget displays log-based alert messages for both the Fortinet unit itself and connected devices.

Alert messages help you track system events on your Fortinet unit such as firmware changes, and network events such as detected attacks. Each message shows the date and time that the event occurred.

Alert messages can also be delivered by email, syslog, or SNMP.

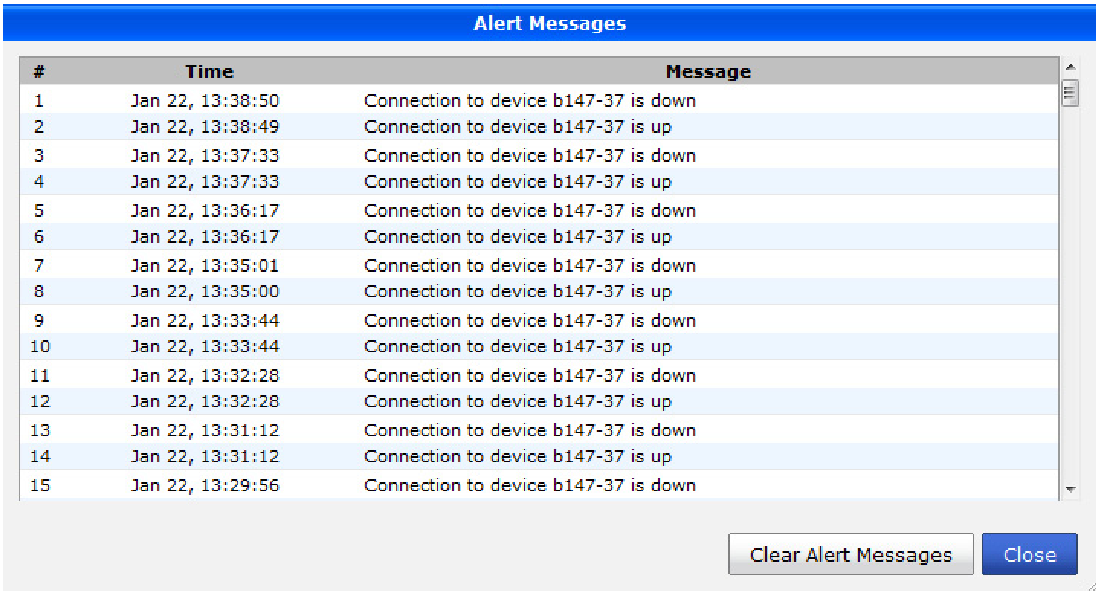
Figure 26: Alert Message Console widget



Time	Message
Jan 22, 13:36:17 -	Connection to device b147-37 is down
Jan 22, 13:36:17 -	Connection to device b147-37 is up
Jan 22, 13:35:01 -	Connection to device b147-37 is down
Jan 22, 13:35:00 -	Connection to device b147-37 is up
Jan 22, 13:33:44 -	Connection to device b147-37 is down
Jan 22, 13:33:44 -	Connection to device b147-37 is up
Jan 22, 13:32:28 -	Connection to device b147-37 is down
Jan 22, 13:32:28 -	Connection to device b147-37 is up
Jan 22, 13:31:12 -	Connection to device b147-37 is down
Jan 22, 13:31:12 -	Connection to device b147-37 is up

The widget displays only the most current alerts. For a complete list of unacknowledged alert messages (see Figure 27), select the *More Alerts* icon in the widget's title bar. A popup window appears. To clear the list, select *Clear Alert Messages*.

Figure 27: List of all alert messages



#	Time	Message
1	Jan 22, 13:38:50	Connection to device b147-37 is down
2	Jan 22, 13:38:49	Connection to device b147-37 is up
3	Jan 22, 13:37:33	Connection to device b147-37 is down
4	Jan 22, 13:37:33	Connection to device b147-37 is up
5	Jan 22, 13:36:17	Connection to device b147-37 is down
6	Jan 22, 13:36:17	Connection to device b147-37 is up
7	Jan 22, 13:35:01	Connection to device b147-37 is down
8	Jan 22, 13:35:00	Connection to device b147-37 is up
9	Jan 22, 13:33:44	Connection to device b147-37 is down
10	Jan 22, 13:33:44	Connection to device b147-37 is up
11	Jan 22, 13:32:28	Connection to device b147-37 is down
12	Jan 22, 13:32:28	Connection to device b147-37 is up
13	Jan 22, 13:31:12	Connection to device b147-37 is down
14	Jan 22, 13:31:12	Connection to device b147-37 is up
15	Jan 22, 13:29:56	Connection to device b147-37 is down

Select the *Edit* icon in the title bar to open the *Edit Alert Message Console Settings* dialog box so that you can adjust the number of entries visible, and their refresh interval.

CLI Console widget

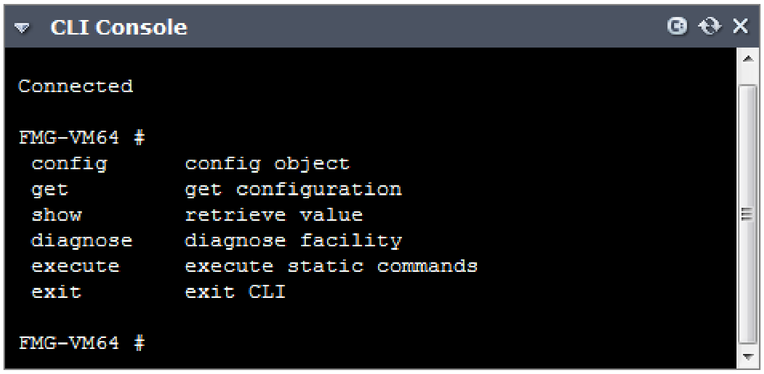
The CLI Console widget enables you to enter command lines through the Web-based Manager, without making a separate Telnet, SSH, or local console connection to access the CLI.

The CLI Console widget requires that your web browser support JavaScript.

To use the console, click within the console area. Doing so will automatically log you in using the same administrator account you used to access the Web-based Manager. You can then enter commands by typing them. You can copy and paste commands into or from the console.

The command prompt, by default the model number such as `Fortinet-800B #`, contains the host name of the Fortinet unit. To change the host name, see "Changing the host name" on page 53.

Figure 28:CLI Console widget



```
Connected

FMG-VM64 #
 config       config object
 get          get configuration
 show         retrieve value
 diagnose     diagnose facility
 execute      execute static commands
 exit         exit CLI

FMG-VM64 #
```

The CLI Console widget can be opened in a new window by selecting the *Detach* icon in the widget's title bar.

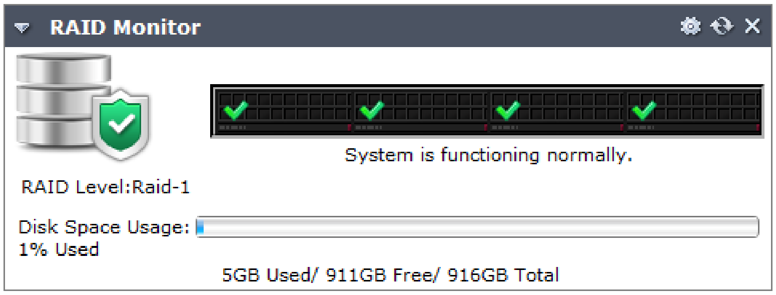
For information on available CLI commands, see the *FortiManager CLI Reference*.

RAID Monitor widget

RAID (Redundant Array of Independent Disks) helps to divide data storage over multiple disks which provides increased data reliability. FortiManager units that contain multiple hard disks can configure the RAID array for capacity, performance, and availability.

You can view the status of the RAID array from the RAID Monitor widget on the *System Settings* > *General* > *Dashboard* page. The RAID Monitor widget displays the status of each disk in the RAID array, including the disk's RAID level. This widget also displays how much disk space is being used.

Figure 29:RAID Monitor widget



RAID Monitor

System is functioning normally.

RAID Level:Raid-1

Disk Space Usage:
1% Used

5GB Used/ 911GB Free/ 916GB Total

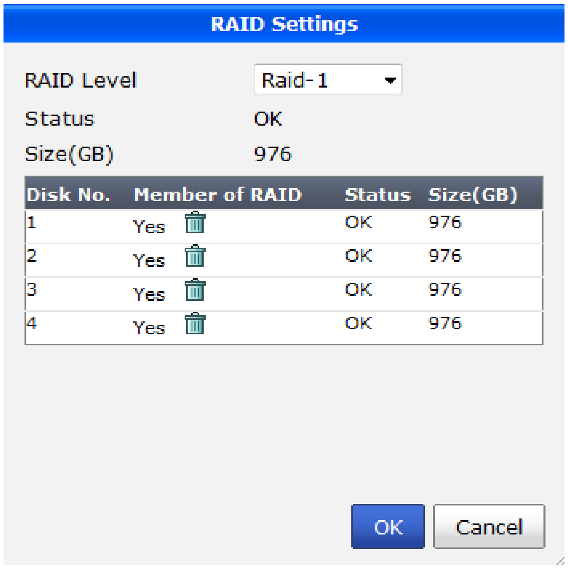
The *Alert Message Console* widget, located in *System Settings> General* > *Dashboard*, will provides detailed information about RAID array failures. For more information see “Alert Messages Console widget” on page 63.

If you need to remove a disk from the FortiManager unit, you might be able to hot swap it. Hot swapping means that you can remove a failed hard disk and replace it with a new one while the FortiManager unit is in operation. Hot swapping is a quick and efficient way to replace hard disks. For more information about hot swapping, see “Hot-swapping hard disks” on page 66.

To configure RAID:

1. Go to *System Settings* > *General* > *Dashboard*.
2. From the RAID Monitor widget title bar, select *RAID Settings*. The RAID Settings dialog box appears.

   Figure 30:RAID Settings

   RAID Settings

   RAID Level: Raid-1

   Status: OK

   Size(GB): 976

Disk No.	Member of RAID	Status	Size(GB)
1	Yes	OK	976
2	Yes	OK	976
3	Yes	OK	976
4	Yes	OK	976

3. From the *RAID Level* list, select the RAID option you want to configure and then select *Apply*. Once selected, depending on the RAID level, it may take a while to generate the RAID array.

Supported RAID levels

FortiManager units with multiple hard drives support the following RAID levels:

- **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, for example:

  - two RAID 1 arrays of two disks each
  - three RAID 1 arrays of two disks each
  - six RAID1 arrays of two disks each.

  One drive from a RAID 1 array can fail without the loss of data; however, should the other drive in the RAID 1 array fail, all data will be lost. In this situation, it is important to replace a failed drive as quickly as possible.

Hot-swapping hard disks

If a hard disk on a FortiManager unit fails, it must be replaced. On FortiManager devices that support hardware RAID, the hard disk can be replaced while the FortiManager unit is running, also known as hot swapping. On FortiManager units with software RAID, the device must be shutdown prior to exchanging the hard disk.

To identify which hard disk failed, read the relevant log message in the *Alert Message Console* widget (see “Alert Message Console widget” on page 63).

To hot-swap a hard disk on a device that supports hardware RAID, simply remove the faulty hard disk and replace it with a new one.:

Electrostatic discharge (ESD) can damage FortiManager equipment. Only perform the procedures described in this document from an ESD workstation. If no such station is available, you can provide some ESD protection by wearing an anti-static wrist or ankle strap and attaching it to an ESD connector or to a metal part of a FortiManager chassis.

When replacing a hard disk, you need to first verify that the new disk has the same size as those supplied by Fortinet and has at least the same capacity as the old one in the FortiManager unit. Installing a smaller hard disk will affect the RAID setup and may cause data loss. Due to possible differences in sector layout between disks, the only way to guarantee that two disks have the same size is to use the same brand and model.

The size provided by the hard drive manufacturer for a given disk model is only an approximation. The exact size is determined by the number of sectors present on the disk.

The FortiManager unit will automatically add the new disk to the current RAID array. The status appears on the console. The widget will display a green check mark icon for all disks and the *RAID Status* area will display the progress of the RAID re-synchronization/rebuild.

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

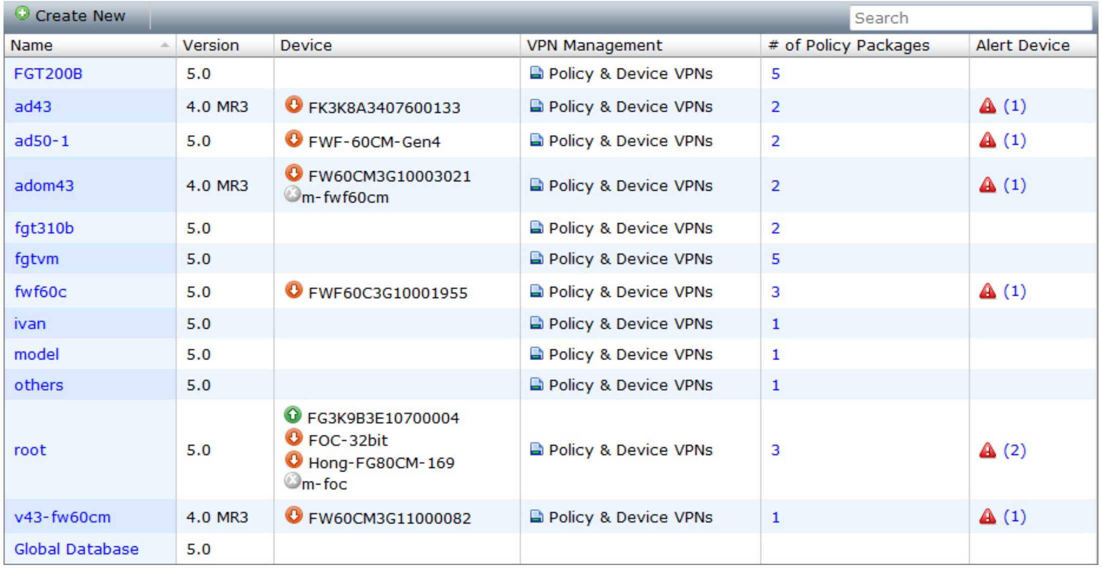
General settings

General settings includes options for the system dashboard, ADOMs, network settings, certificates, high availability, log access, and diagnostic tools.

All ADOMS

To view a listing of all the ADOMs and to create new ADOMs, go to *System Settings* > *General* > *All ADOMs*.

Figure 31: All ADOMs



Create New

Search

Name	Version	Device	VPN Management	# of Policy Packages	Alert Device
FGT200B	5.0		Policy & Device VPNs	5	
ad43	4.0 MR3	FK3K8A3407600133	Policy & Device VPNs	2	⚠ (1)
ad50-1	5.0	FWF-60CM-Gen4	Policy & Device VPNs	2	⚠ (1)
adom43	4.0 MR3	FW60CM3G10003021 m-fwf60cm	Policy & Device VPNs	2	⚠ (1)
fgt310b	5.0		Policy & Device VPNs	2	
fgtvm	5.0		Policy & Device VPNs	5	
fwf60c	5.0	FWF60C3G10001955	Policy & Device VPNs	3	⚠ (1)
ivan	5.0		Policy & Device VPNs	1	
model	5.0		Policy & Device VPNs	1	
others	5.0		Policy & Device VPNs	1	
root	5.0	FG3K9B3E10700004 FOC-32bit Hong-FG80CM-169 m-foc	Policy & Device VPNs	3	⚠ (2)
v43-fw60cm	4.0 MR3	FW60CM3G11000082	Policy & Device VPNs	1	⚠ (1)
Global Database	5.0				

Create New	Select to create a new ADOM. For information on creating a new ADOM, see "Adding an ADOM" on page 44
Name	The ADOM name.
Version	The ADOM version.
Device	The device or devices that the ADOM contains.
VPN Management	VPN management information for the ADOM.
# of Policy Packages	The number of policy packages currently used by the ADOM. Select the number to view a list of the policy packages and their installation targets.
Alert Device	The number of devices in the ADOM that currently have alerts. Select the number to view a list of the devices with alerts and the alert details.

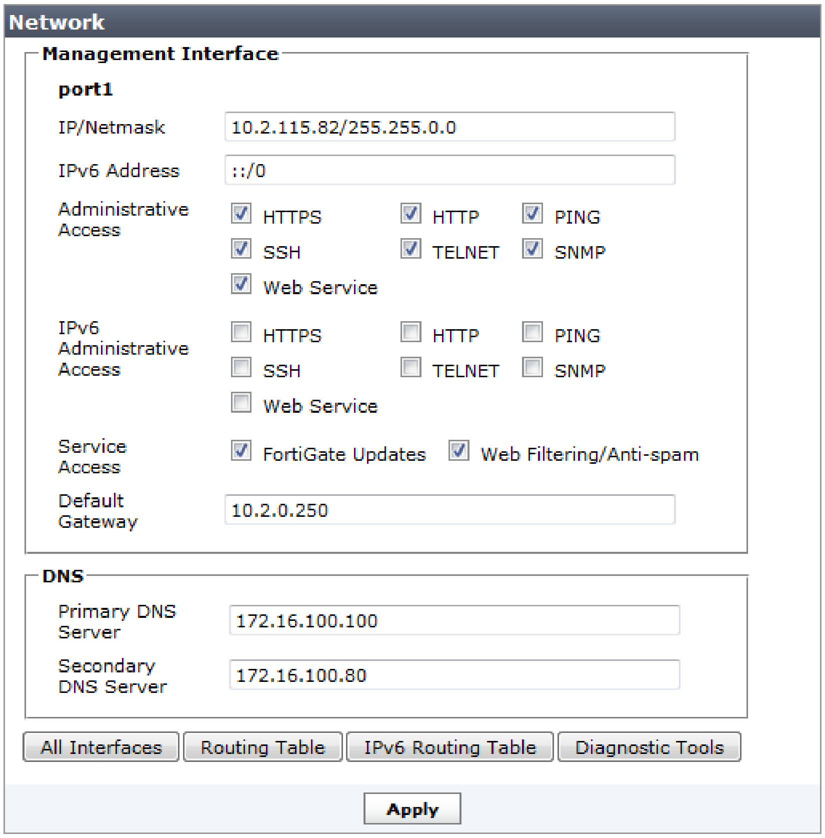
The ADOMs in the list can also be edited and deleted as required. See "Managing ADOMs" on page 43 for more information.

Network

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

To view the configured network interfaces, go to *System Settings* > *General* > *Network*. The Network screen is displayed.

Figure 32: Network screen



Network

Management Interface

port1

IP/Netmask: 10.2.115.82/255.255.0.0

IPv6 Address: ::/0

Administrative Access: ☑ HTTPS ☑ HTTP ☑ PING ☑ SSH ☑ TELNET ☑ SNMP ☑ Web Service

IPv6 Administrative Access: □ HTTPS □ HTTP □ PING □ SSH □ TELNET □ SNMP □ Web Service

Service Access: ☑ FortiGate Updates ☑ Web Filtering/Anti-spam

Default Gateway: 10.2.0.250

DNS

Primary DNS Server: 172.16.100.100

Secondary DNS Server: 172.16.100.80

The following information is available:

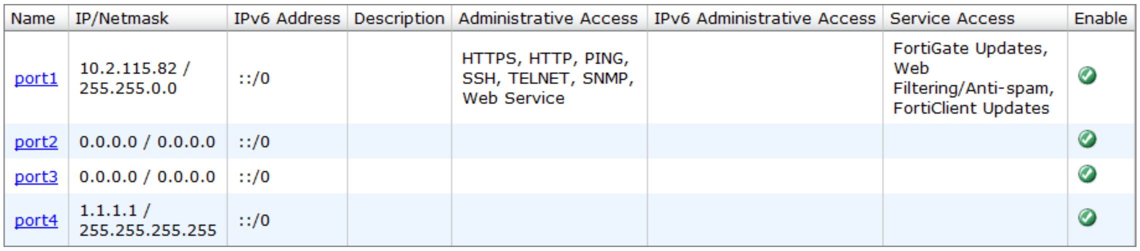
Management Interface	
IP/Netmask	The IP address and netmask associated with this interface.
IPv6 Address	The IPv6 address associated with this interface.
Administrative Access	Select the allowed administrative service protocols from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, and Web Service.
IPv6 Administrative Access	Select the allowed IPv6 administrative service protocols from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, and Web Service.
Service Access	Select the Fortinet services that are allowed access on this interface. These include FortiGate updates and web filtering /email filtering. By default all service access is enabled on port1, and disabled on port2.

Default Gateway	The default gateway associated with this interface
DNS	
Primary DNS Server	Enter the primary DNS server IP address.
Secondary DNS Server	Enter the secondary DNS server IP address.
All Interfaces	Click to open the network interface list. See "Viewing the network interface list" on page 70.
Routing Table	Click to open the routing table. See "Configuring static routes" on page 72.
IPv6 Routing Table	Click to open the IPv6 routing table. See "Configuring IPv6 static routes" on page 73.
Diagnostic Tools	Select to run available diagnostic tools, including *Ping*, *Traceroute*, and *View logs*.

Viewing the network interface list

To view the network interface list, select the *All Interfaces* button.

Figure 33: Network interface list



Name	IP/Netmask	IPv6 Address	Description	Administrative Access	IPv6 Administrative Access	Service Access	Enable
port1	10.2.115.82 / 255.255.0.0	::/0		HTTPS, HTTP, PING, SSH, TELNET, SNMP, Web Service		FortiGate Updates, Web Filtering/Anti-spam, FortiClient Updates	✓
port2	0.0.0.0 / 0.0.0.0	::/0					✓
port3	0.0.0.0 / 0.0.0.0	::/0					✓
port4	1.1.1.1 / 255.255.255.255	::/0					✓

The following information is available:

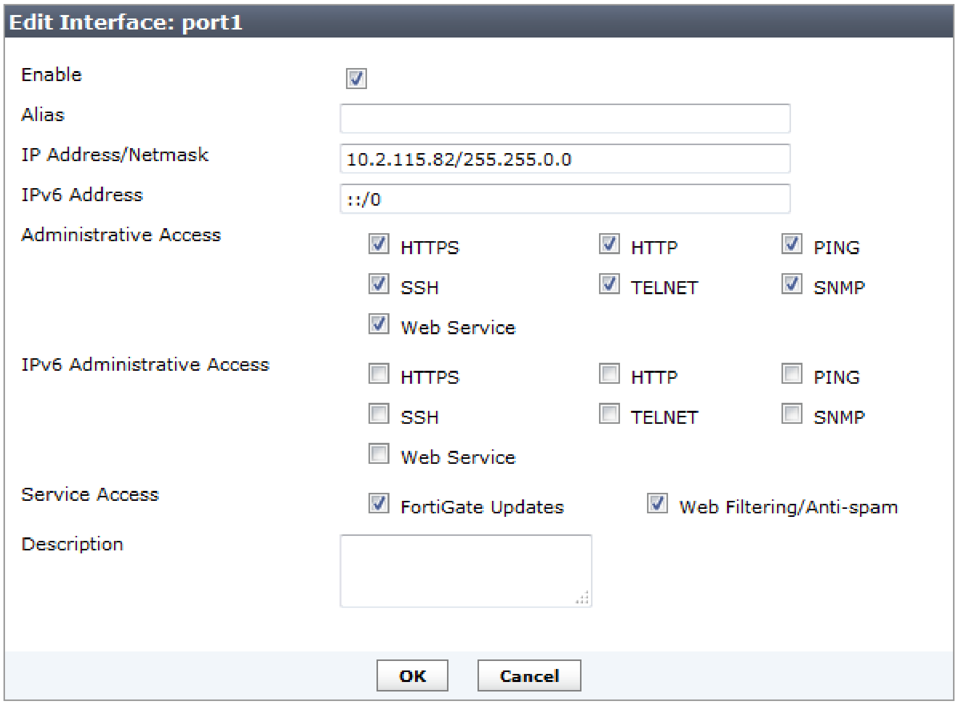
Name	The names of the physical interfaces on your FortiManager unit. The name, including number, of a physical interface depends on the model. Unlike FortiGate, you cannot set alias names for the interfaces. For more information, on configuring the interface, see "Configuring network interfaces" on page 71. 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.
IPv6 Address	The IPv6 address associated with this interface.
Description	A description of the interface.
Administrative Access	The list of allowed administrative service protocols on this interface. These include HTTP, HTTPS, PING, SSH, and Telnet.
IPV6 Administrative access	The list of allowed IPv6 administrative service protocols on this interface.

Service Access	The list of Fortinet services that are allowed access on this interface. These include FortiGate updates, web filtering, and email filter. 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.

Configuring network interfaces

In the Network interface list select the interface name link to change the interface options.

Figure 34: Configure network interfaces



Edit Interface: port1

Enable ☑

Alias

IP Address/Netmask 10.2.115.82/255.255.0.0

IPv6 Address ::/0

Administrative Access ☑ HTTPS ☑ HTTP ☑ PING ☑ SSH ☑ TELNET ☑ SNMP ☑ Web Service

IPv6 Administrative Access □ HTTPS □ HTTP □ PING □ SSH □ TELNET □ SNMP □ Web Service

Service Access ☑ FortiGate Updates ☑ Web Filtering/Anti-spam

Description

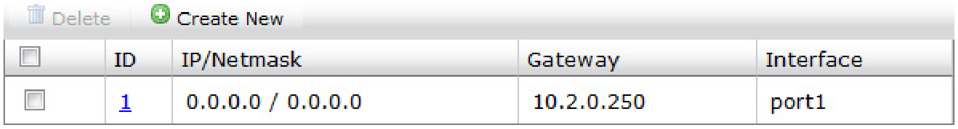
Enable	Select to enable this interface. A green circle with a check mark appears in the interface list to indicate the interface is accepting network traffic. When not selected, a gray circle with an “X” appears in the interface list to indicate the interface is down and not accepting network traffic.
Alias	Enter an alias for the port to make it easily recognizable.
IP Address/Netmask	Enter the IP address and netmask for the interface.
IPv6 Address	Enter the IPv6 address for the interface.
Administrative Access	Select the services to allow on this interface. Any interface that is used to provide administration access to the FortiManager unit will require at least HTTPS or HTTP for web-manager access, or SSH for CLI access.

IPv6 Administrative Access	Select the services to allow on this interface.
Service access	Select the services that will communicate with this interface.
Description	Enter a brief description of the interface (optional).

Configuring static routes

Go to *System Settings* > *General* > *Network* and select the *Routing Table* button 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 35: Routing table



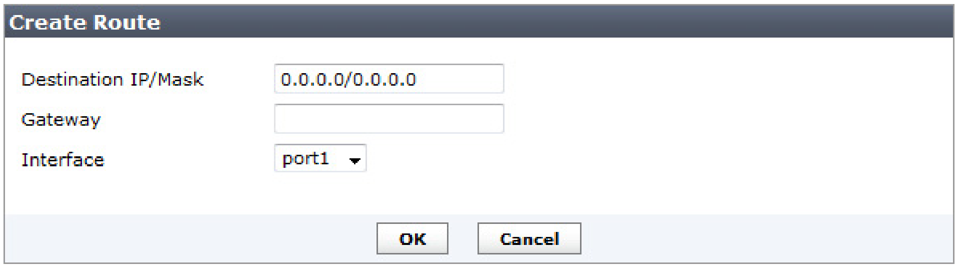
☐	ID	IP/Netmask	Gateway	Interface
☐	1	0.0.0.0 / 0.0.0.0	10.2.0.250	port1

Delete	Select the check box next to the route number and select *Delete* to remove the route from the table.
Create New	Select *Create New* to add a new route. See "Add a static route" on page 72. Select the route number to edit the settings.
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.

Add a static route

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

Figure 36: Create new route



Destination IP/Mask	0.0.0.0/0.0.0.0
Gateway	
Interface	port1

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 IPv6 static routes

Go to *System Settings* > *General* > *Network* and select the *IPv6 Routing Table* button to view, edit, or add to the IPv6 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.

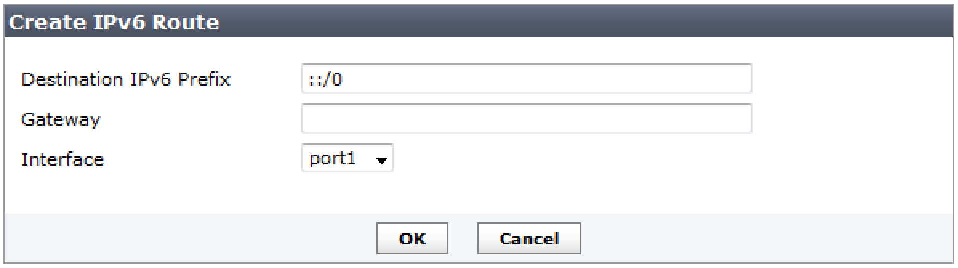
The following information and settings are available:

Delete	Select the check box next to the route number and select *Delete* to remove the route from the table.
Create New	Select *Create New* to add a new route. See "Add a IPv6 static route" on page 73. Select the route number to edit the settings.
ID	The route number.
IPv6 Address	The destination IPv6 address 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.

Add a IPv6 static route

Go to *System Settings* > *General* > *Network,* select the *IPv6 Routing Table* button**,** and select *Create New* to add a route, or select the route number to edit an existing route.

Figure 37: Create new IPv6 route



Create IPv6 Route

Destination IPv6 Prefix: ::/0

Gateway:

Interface: port1

Destination IPv6 Prefix	Enter the destination IPv6 prefix 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.

Certificates

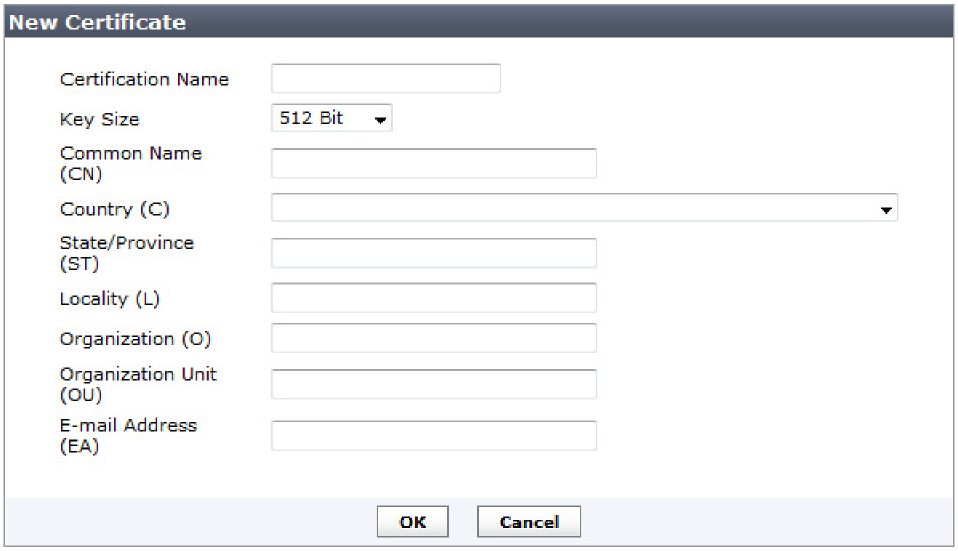
The FortiManager unit generates a certificate request based on the information you enter to identify the FortiManager unit. After you generate a certificate request, you can download the request to a computer that has management access to the FortiManager unit and then forward the request to a CA.

Creating a local certificate

To create a certificate request:

1. Go to *System Settings* > *General* > *Certificates* > *Local Certificates*.
2. Select the *Create New* button and enter the information as required and select *Ok*.

Figure 38: New local certificate



New Certificate

Certification Name	
Key Size	512 Bit
Common Name (CN)	
Country (C)	
State/Province (ST)	
Locality (L)	
Organization (O)	
Organization Unit (OU)	
E-mail Address (EA)	

Certificate Name	The name of the certificate.
Key Size	Select the key size from the drop-down list.
Common Name (CN)	Enter the common name of the certificate.
Country (C)	Select the country from the drop-down list.
State/Province (ST)	Enter the state or province.
Locality (L)	Enter the locality.
Organization (O)	Enter the organization for the certificate.
Organization Unit (OU)	Enter the organization unit.
E-mail Address (EA)	Enter the email address.

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

Only Local Certificates can be created. CA Certificates can only be imported

Importing certificates

To import a local certificate:

1. Go to *System Settings* > *General* > *Certificates* > *Local Certificates*.
2. Select the *Import* button.
3. Enter the location of the local certificate, or select *browse* and browse to the location of the certificate, and select *Ok*.

To import a CA certificate:

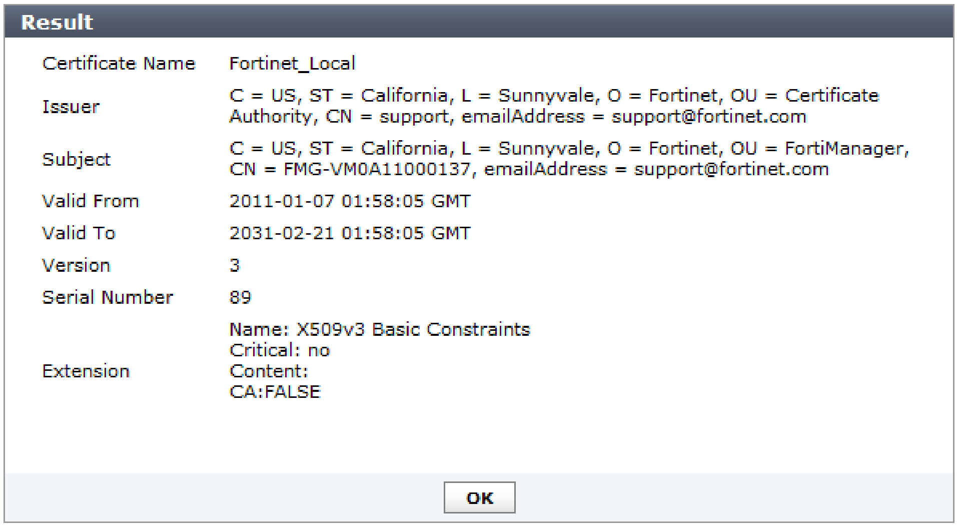
1. Go to *System Settings* > *General* > *Certificates* > *CA Certificates*.
2. Select the *Import* button.
3. Enter the location of the local certificate, or select *browse* and browse to the location of the certificate, and select *Ok*.

Viewing certificate details

To view a local certificate:

1. Go to *System Settings* > *General* > *Certificates* > *Local Certificates*.
2. Select the certificates which you would like to see details about and click on *View Certificate Detail*.

Figure 39: Local certificate detail



Result

Certificate Name	Fortinet_Local
Issuer	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortinet.com
Subject	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiManager, CN = FMG-VM0A11000137, emailAddress = support@fortinet.com
Valid From	2011-01-07 01:58:05 GMT
Valid To	2031-02-21 01:58:05 GMT
Version	3
Serial Number	89
Extension	Name: X509v3 Basic Constraints Critical: no Content: CA:FALSE

Certificate Name	The name of the certificate.
Issuer	The issuer of the certificate.

Subject	The subject of the certificate.
Valid From	The date from which the certificate is valid.
Valid To	The last day that the certificate is valid. The certificate should be renewed before this date.
Version	The certificate’s version.
Serial Number	The serial number of the certificate.
Extension	The certificate extension information.

To view a CA certificate:

1. Go to *System Settings* > *General* > *Certificates* > *CA Certificates*.
2. Select the certificates which you would like to see details about and click on *View Certificate Detail*.

   The details displayed are similar to those displayed for a local certificate.

Downloading a certificate

To download a local certificate:

1. Go to *System Settings* > *General* > *Certificates* > *Local Certificates*.
2. Select the certificates which you would like to download, click on *Download*, and save the certificate to the desired location.

To download a CA certificate:

1. Go to *System Settings* > *General* > *Certificates* > *CA Certificates*.
2. Select the certificates which you would like to download, click on *Download*, and save the certificate to the desired location.

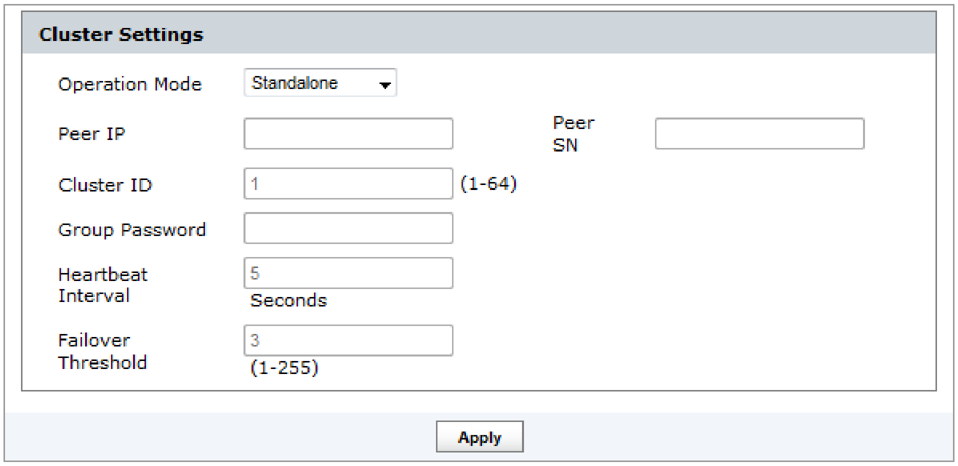
High Availability

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.

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.

Figure 40: Cluster settings dialog box



Cluster Settings

Operation Mode	Standalone		
Peer IP		Peer SN	
Cluster ID	1 (1-64)		
Group Password			
Heartbeat Interval	5 Seconds		
Failover Threshold	3 (1-255)		

To configure a cluster, you must set the mode of the primary unit to Master and the modes of the backup units to Slave.

Then you must add the IP addresses and serial numbers of each backup unit to primary unit peer list. The IP address and serial number of the primary unit must be added to each of the backup unit HA configurations. Also, the primary unit and all backup units must have the same *Cluster ID* and *Group Password*.

You can connect to the primary unit 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.

When the cluster is operating, from the primary unit Web-based Manager you can change HA settings. For example you might want to change the heartbeat interval and failover threshold to fine tune the failure detection time. You should also change the password and Cluster ID to be different from the default settings.

For more information on High Availability, see “High Availability” on page 297.

Log access

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 the log messages:

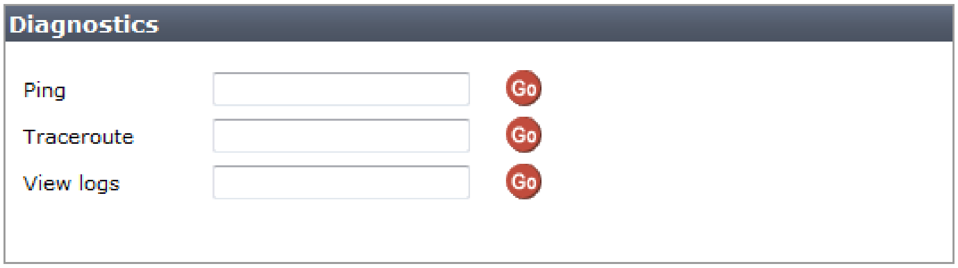
1. Go to *System Settings* > *General* > *Log Access*.
2. Select the log type by selecting it from the *Type* drop-down list on the toolbar.

3. Select *Clear Filter* to clear any column filters in the list.
4. Select *Column Settings* to adjust the column settings for the list.
5. Select *Download* to download a file containing the logs in either CSV or the normal format.
6. Select the *Raw Log/Formatted Table* button to toggle log message view.
7. Select *Refresh* to refresh the displayed logs.
8. Select *Historical Log* to view historical logs.

Diagnostic tools

Diagnostic tools allows you to run available diagnostic tools, including *Ping*, *Traceroute*, and *View logs*.

Figure 41: Diagnostic tools



Admin

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

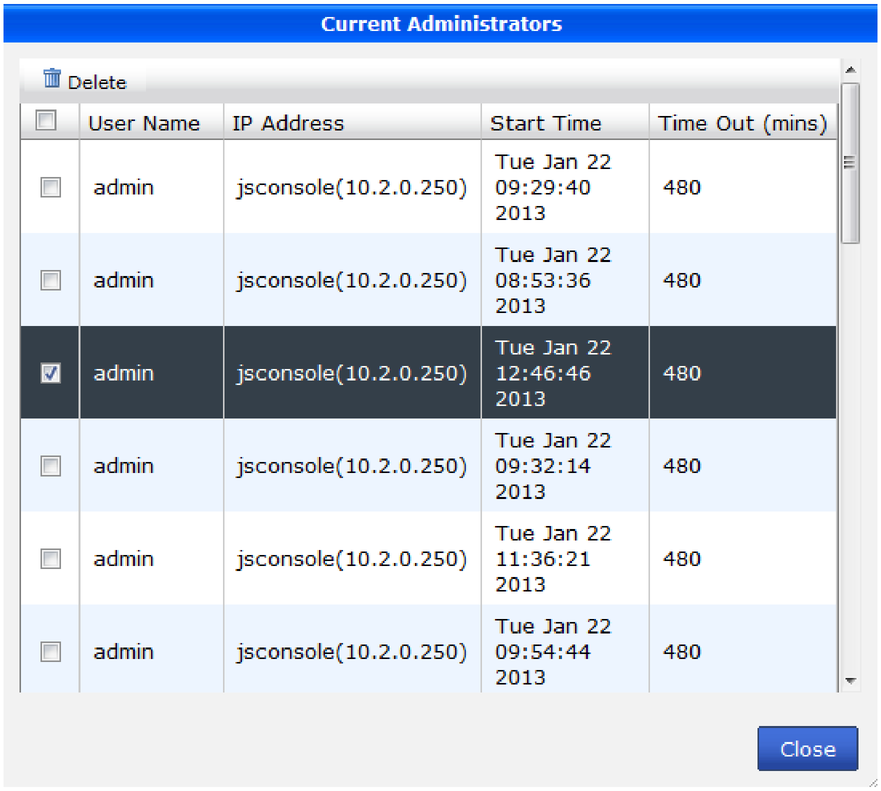
Administrator	Select to configure administrative users accounts. For more information, see “Administrator” on page 80.
Profile	Select to set up access profiles for the administrative users. For more information, see “Profile” on page 83.
Remote Auth Server	Select to configure authentication server settings for administrative log in. For more information, see “Remote authentication server” on page 86.
Admin Settings	Select to configure connection options for the administrator including port number, language of the Web-based Manager and idle timeout. For more information, see “Administrator settings” on page 90.

Monitoring administrator sessions

The *Current Administrators* view enables you to view the list of administrators logged into the FortiManager unit. From this window you can also disconnect users if necessary.

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

Figure 42: Administrator session list



Current Administrators

☐	User Name	IP Address	Start Time	Time Out (mins)
☐	admin	jsconsole(10.2.0.250)	Tue Jan 22 09:29:40 2013	480
☐	admin	jsconsole(10.2.0.250)	Tue Jan 22 08:53:36 2013	480
☑	admin	jsconsole(10.2.0.250)	Tue Jan 22 12:46:46 2013	480
☐	admin	jsconsole(10.2.0.250)	Tue Jan 22 09:32:14 2013	480
☐	admin	jsconsole(10.2.0.250)	Tue Jan 22 11:36:21 2013	480
☐	admin	jsconsole(10.2.0.250)	Tue Jan 22 09:54:44 2013	480

The following information is available:

User Name	The name of the administrator account. Your session is indicated by *(current)*.
IP Address	The IP address where the administrator is logging in from.
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* > *General* > *Dashboard*.
2. In the System Information widget, under *Current Administrators*, select *Detail*. The list of current administrator sessions appears; see Figure 42.
3. Select the check box for each administrator session that you want to disconnect, and select *Delete*.

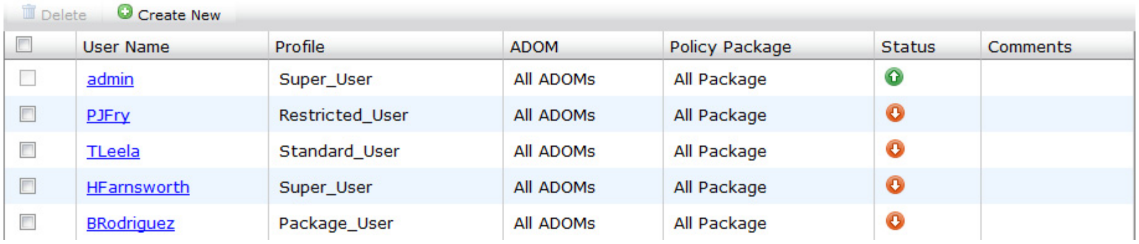
4. Select *OK* to confirm deletion of the session.

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.

Administrator

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

Figure 43: Administrator list



□	User Name	Profile	ADOM	Policy Package	Status	Comments
□	admin	Super_User	All ADOMs	All Package	↑	
□	PJFry	Restricted_User	All ADOMs	All Package	↓	
□	TLeela	Standard_User	All ADOMs	All Package	↓	
□	HFarnsworth	Super_User	All ADOMs	All Package	↓	
□	BRodriguez	Package_User	All ADOMs	All Package	↓	

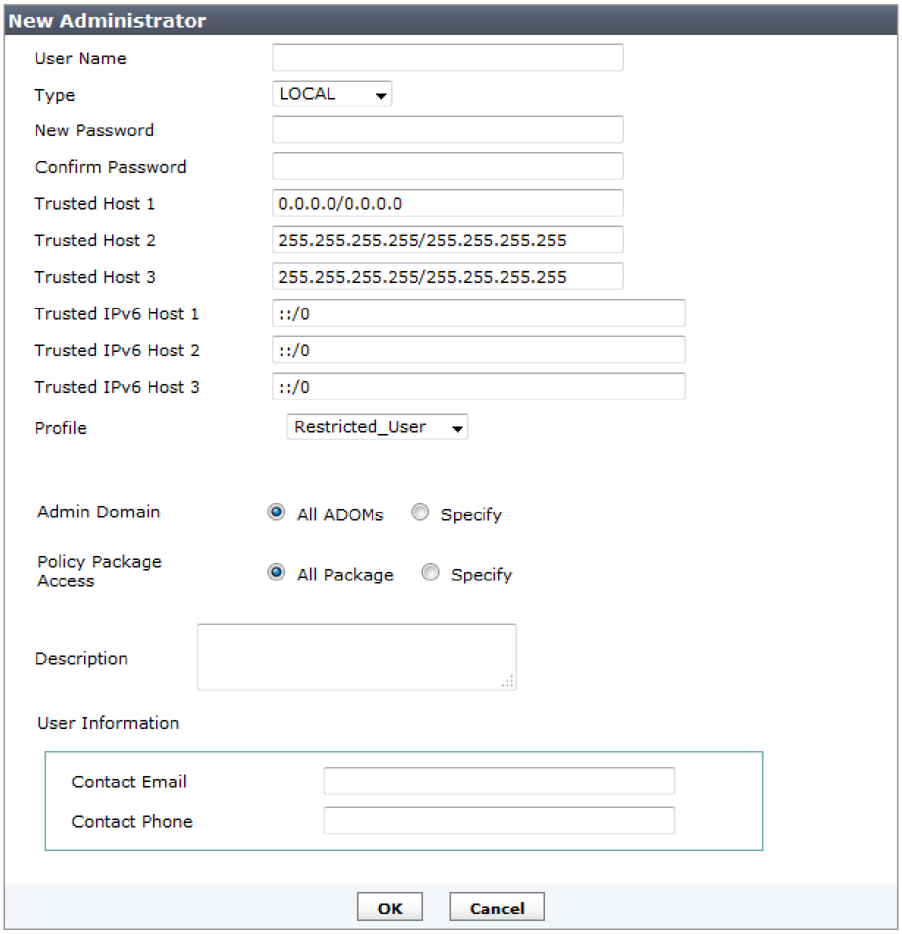
The following information is available:

Delete	Select the check box next to the administrator you want to remove from the list and select *Delete*.
Create New	Select to create a new administrator. For more information, see "To create a new administrator account:" on page 81.
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 "Profile" on page 83.
ADOM	The ADOM to which the administrator has been assigned.
Policy Package	The policy packages to which this profile allows access.
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.

To create a new administrator account:

1. Go to *System Settings* > *Admin* > *Administrator* and select *Create New*. The *New Administrator* dialog box appears; see Figure 44.

Figure 44: Creating a new administrator account



New Administrator

User Name	
Type	LOCAL
New Password	
Confirm Password	
Trusted Host 1	0.0.0.0/0.0.0.0
Trusted Host 2	255.255.255.255/255.255.255.255
Trusted Host 3	255.255.255.255/255.255.255.255
Trusted IPv6 Host 1	::/0
Trusted IPv6 Host 2	::/0
Trusted IPv6 Host 3	::/0
Profile	Restricted_User
Admin Domain	● All ADOMs ○ Specify
Policy Package Access	● All Package ○ Specify
Description	

User Information

Contact Email	
Contact Phone	

2. Configure the following 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.
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 83.
Trusted IPv6 Host1 **Trusted IPv6 Host2** **Trusted IPv6 Host3**	Optionally, enter the trusted host IPv6 address from which the administrator can log in to the FortiManager unit. You can specify up to three trusted IPv6 hosts. Setting trusted IPv6 hosts for all of your administrators can enhance the security of your system. For more information, see "Using trusted hosts" on page 83.
Profile	Select a profile from the list. The profile selected determines the administrator's access to the FortiManager unit's features. To create a new profile see "Configuring administrator profiles" on page 85.
Admin Domain	Choose the ADOM this admin will belong to, or select *All ADOMs*. This field is available only if ADOMs are enabled.
Policy Package Access	Choose the policy packages this admin will have access to, or select *All Package*.
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.
User Information (optional)	
Contact Email	Enter a contact email address for the new administrator.
Contact Phone	Enter a contact phone number for the new administrator.

3. Select *OK* to create the new administrator account.

To modify an existing administrator account:

1. Go to *System Settings > Admin> Administrator.* The list of configured administrators appears; see Figure 43 on page 80.
2. In the *User Name* column, double-click on the user name of the administrator you want to change. The *Edit Administrator* window appears.
3. Modify the settings as required. For more information about configuring account settings, see "To create a new administrator account:" on page 81.
4. Select *OK* to save your changes.

To delete an existing administrator account:

1. Go to *System Settings > Admin > Administrator.* The list of configured administrators appears; see Figure 43 on page 80.
2. Select the check box of the administrator account you want to delete and then select the *Delete* icon in the toolbar.
3. In the dialog box that appears, select *OK* to confirm the deletion.

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.

If you set trusted hosts and want to use the Console Access feature of the Web-based Manager, you must also set 127.0.0.1/255.255.255.255 as a trusted host. By default, Trusted Host 3 is set to this address.

Profile

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

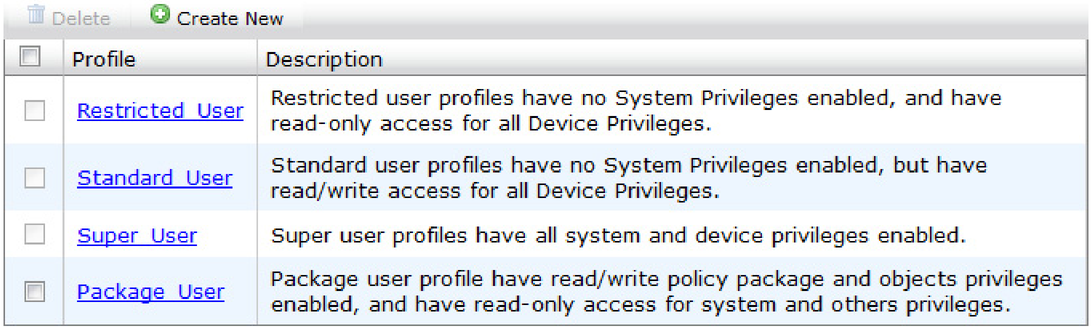
Restricted_User	Restricted user profiles have no System Privileges enabled, and have read-only access for all Device Privileges.
Standard_User	Standard user profiles have no System Privileges enabled, but have read/write access for all Device Privileges.
Super_User	Super user profiles have all system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

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

This Guide is intended for default users with full 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.

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

Figure 45: Administrator profile list



□	Profile	Description
□	Restricted_User	Restricted user profiles have no System Privileges enabled, and have read-only access for all Device Privileges.
□	Standard_User	Standard user profiles have no System Privileges enabled, but have read/write access for all Device Privileges.
□	Super_User	Super user profiles have all system and device privileges enabled.
□	Package_User	Package user profile have read/write policy package and objects privileges enabled, and have read-only access for system and others privileges.

The default administrator profiles can not be deleted. They can, however, be edited.

The following information is available:

Delete	Select the check box next to the profile you want to delete and select *Delete*. Predefined profiles cannot be deleted. You can only delete custom profiles when they are not applied to any administrators.
Create New	Select to create a custom administrator profile. See "Configuring administrator profiles" on page 85.
Profile	The administrator profile name. Select the profile name to view or modify existing settings. For more information about profile settings, see "Configuring administrator profiles" on page 85.
Description	Provides a brief description of the system and device access privileges allowed for the selected profile.

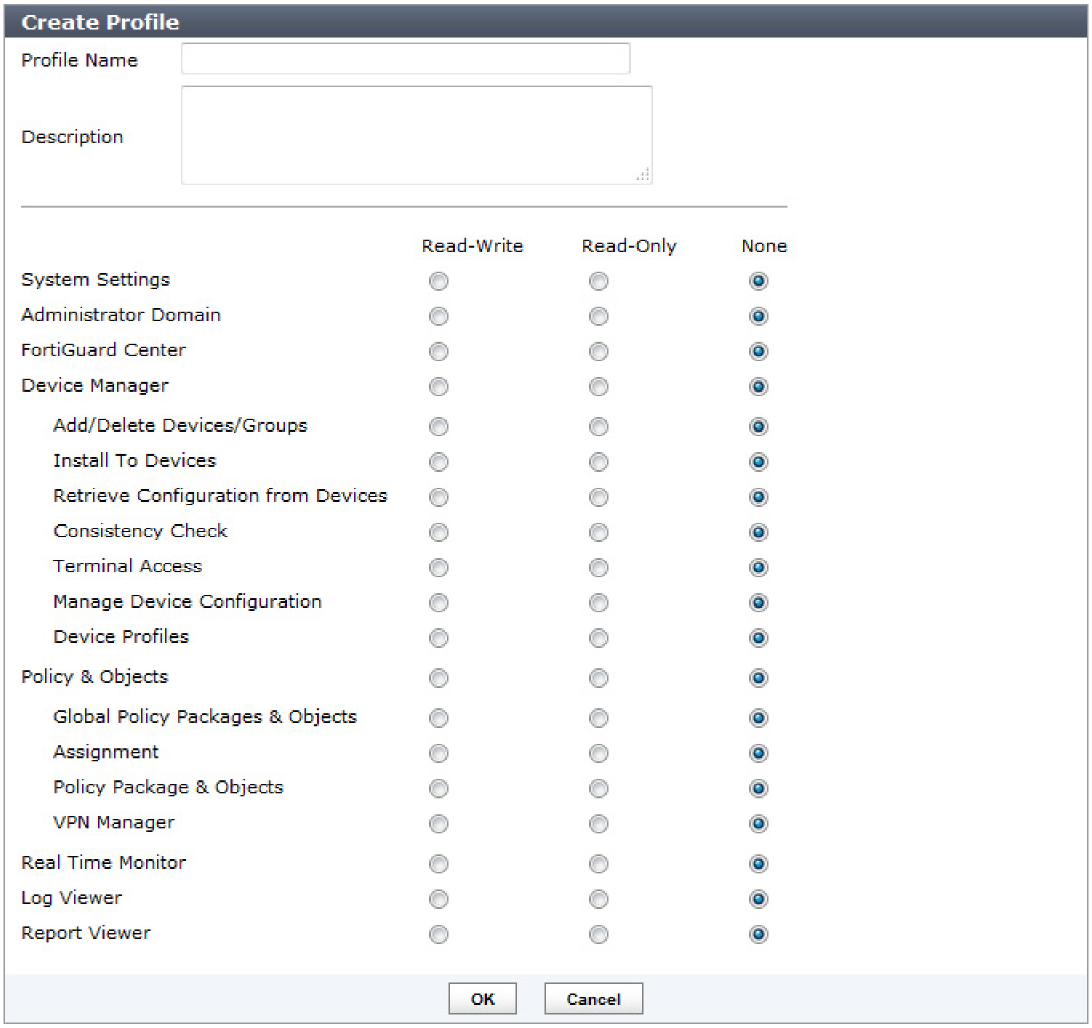
Configuring administrator profiles

You can modify one of the pre-defined profiles or create a custom profile if needed. Only administrators with full system privileges can modify the administrator profiles.

To create a custom profile:

1. Go to *System Settings* > *Admin* > *Profile* and select *Create New*. The *Create Profile* dialog box appears.

Figure 46: Create new administrator profile



Create Profile

Profile Name

Description

	Read-Write	Read-Only	None
System Settings	○	○	●
Administrator Domain	○	○	●
FortiGuard Center	○	○	●
Device Manager	○	○	●
Add/Delete Devices/Groups	○	○	●
Install To Devices	○	○	●
Retrieve Configuration from Devices	○	○	●
Consistency Check	○	○	●
Terminal Access	○	○	●
Manage Device Configuration	○	○	●
Device Profiles	○	○	●
Policy & Objects	○	○	●
Global Policy Packages & Objects	○	○	●
Assignment	○	○	●
Policy Package & Objects	○	○	●
VPN Manager	○	○	●
Real Time Monitor	○	○	●
Log Viewer	○	○	●
Report Viewer	○	○	●

2. Configure the following 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.
System Settings	Select *None*, *Read Only*, or *Read-Write* access.
Administrator Domain	Select *None*, *Read Only*, or *Read-Write* access.

Device Manager	Select *None*, *Read Only*, or *Read-Write* access for categories as required.
Policy & Objects	Select *None*, *Read Only*, or *Read-Write* access for categories as required.
Real Time Monitor	Select *None*, *Read Only*, or *Read-Write* access.
Log Viewer	Select *None*, *Read Only*, or *Read-Write* access.
Report Viewer	Select *None*, *Read Only*, or *Read-Write* access.

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

To modify an existing profile:

1. Go to *System Settings* > *Admin* > *Profile*.
2. In the *Profile* column, double-click on the name of the profile you want to change. The *Edit Profile* dialog box appears, containing the same information as when creating a new profile.
3. Configure the appropriate changes and then select *OK* to save the settings.

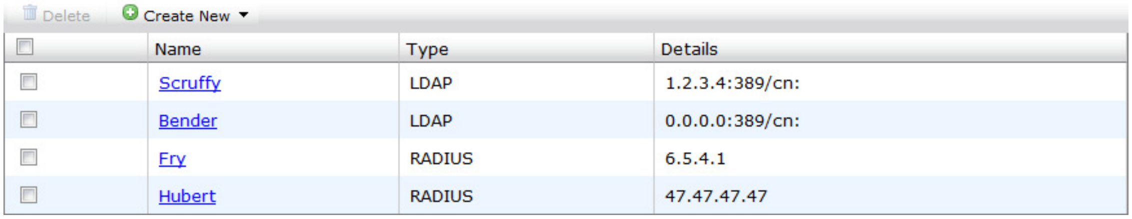
To delete a profile:

1. Go to *System Settings* > *Admin* > *Profile*.
2. Select the check box of the custom profile you want to delete and then select the *Delete* icon in the toolbar. You can only delete custom profiles when they are not applied to any administrators.
3. In the confirmation dialog box that appears, select *OK* to delete the profile.

Remote authentication server

The FortiManager system supports remote authentication of administrators using LDAP, RADIUS, and TACACS+ servers. To use this feature, you must configure the appropriate server entries in the FortiManager unit for each authentication server in your network. New remote authentication servers can be added. Existing servers can be modified and deleted as required; see “Manage remote authentication servers” on page 90.

Figure 47: Remote authentication server list



□	Name	Type	Details
□	Scruffy	LDAP	1.2.3.4:389/cn:
□	Bender	LDAP	0.0.0.0:389/cn:
□	Fry	RADIUS	6.5.4.1
□	Hubert	RADIUS	47.47.47.47

Delete	Delete the selected server.
Create New	Create a new server. Select one of LDAP, RADIUS, or TACACS+ from the drop-down list.
Name	The name of the server.

Type	The server type. One of LDAP, RADIUS, or TACACS+.
Details	Details about the server, such as the IP address.

LDAP

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.

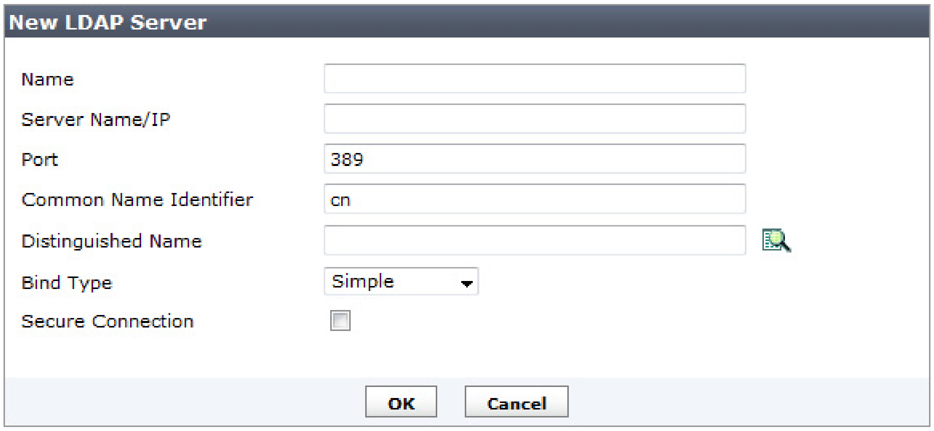
If you have configured LDAP support and require a user to authenticate using an LDAP server, the FortiManager unit contacts the LDAP server for authentication. To authenticate with the FortiManager unit, the user enters a user name and password. The FortiManager unit sends this user name and password 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.

To add an LDAP server:

1. Go to *System Settings > Admin > Remote Auth Server*. The list of servers is shown.
2. Select the *Create New* toolbar icon, then select *LDAP* from the drop-down list.

   The *New LDAP Server* window opens.

   Figure 48: New LDAP server dialog box



New LDAP Server

Name

Server Name/IP

Port 389

Common Name Identifier cn

Distinguished Name

Bind Type Simple

Secure Connection □

3. Configure the following information:

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	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.

Bind Type	Select the type of binding for LDAP authentication.
Secure Connection	Select to use a secure LDAP server connection for authentication.

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

RADIUS

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 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.

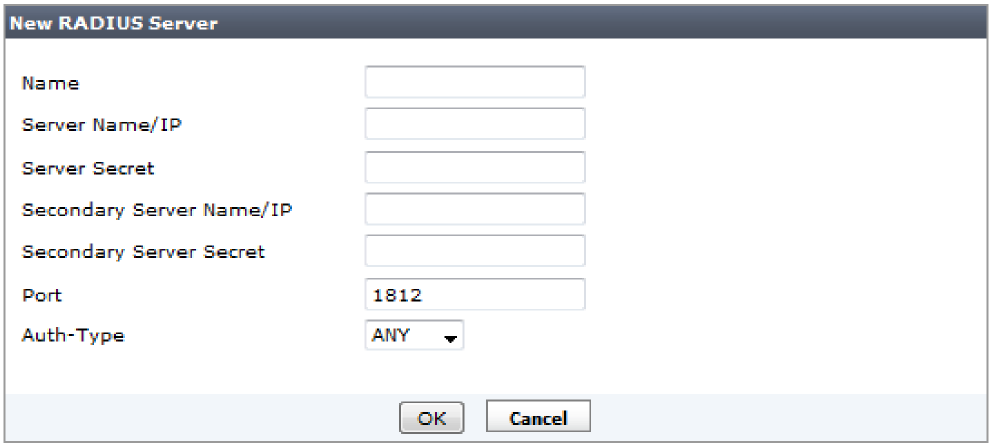
To add a RADIUS server:

1. Go to *System Settings > Admin > Remote Auth Server*.

2. Select the *Create New* toolbar icon, then select *RADIUS* from the drop-down list.

The *New RADIUS Server* window opens.

Figure 49: New RADIUS Server window



New RADIUS Server

Name	
Server Name/IP	
Server Secret	
Secondary Server Name/IP	
Secondary Server Secret	
Port	1812
Auth-Type	ANY

3. Configure the following settings:

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.

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

TACACS+

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.

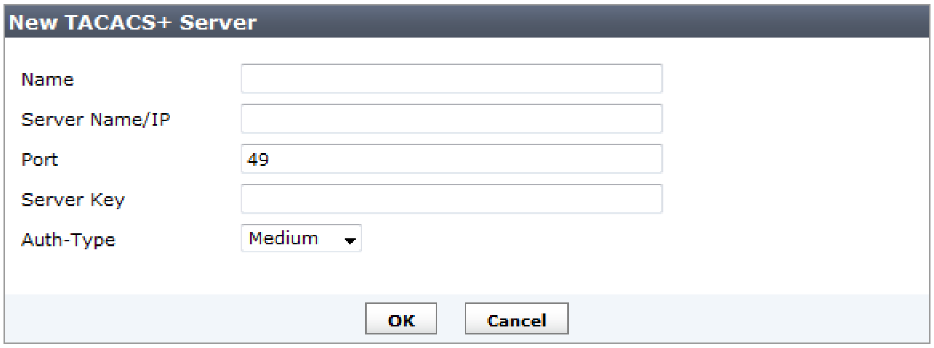
For more information about TACACS servers, see the FortiGate documentation.

To add a TACACS+ server:

1. Go to *System Settings > Admin > Remote Auth Server*.
2. Select the *Create New* toolbar icon, then select *TACACS+* from the drop-down list.

   The *New TACACS+ Server* window opens.

Figure 50: New TACACS+ server dialog box



New TACACS+ Server

Name

Server Name/IP

Port: 49

Server Key

Auth-Type: Medium

3. Configure the following information:

Name	Enter a name to identify the TACACS+ server.
Server Name/IP	Enter the IP address or fully qualified domain name of the TACACS+ server.
Port	Enter the port for TACACS+ traffic. The default port is 389.
Server Key	Enter the key to access the TACACS+ server. The server key can be a maximum of 16 characters in length.
Auth-Type	Enter the authentication type the TACACS+ server requires. The default setting of *ANY* has the FortiManager unit try all the authentication types.

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

Manage remote authentication servers

Remote authentication servers can be modified and deleted as required.

To modify an existing server configuration:

1. Go to *System Settings* > *Admin* > *Remote Auth Server*.
2. In the *Name* column, select the name of the server configuration you want to change. The appropriate edit dialog box will appear for the type of server selected.
3. Modify the settings as required and select *OK* to apply your changes.

To delete an existing server configuration:

1. Go to *System Settings* > *Admin* > *Remote Auth Server*.
2. Select the check box beside the server configuration you want to delete and then select the *Delete* toolbar icon.
3. Select *OK* in the confirmation dialog box to delete the server entry.

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

Administrator settings

The *System Settings* > *Admin* > *Admin Settings* page allows you to configure global settings for administrator access to the FortiManager unit, including:

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

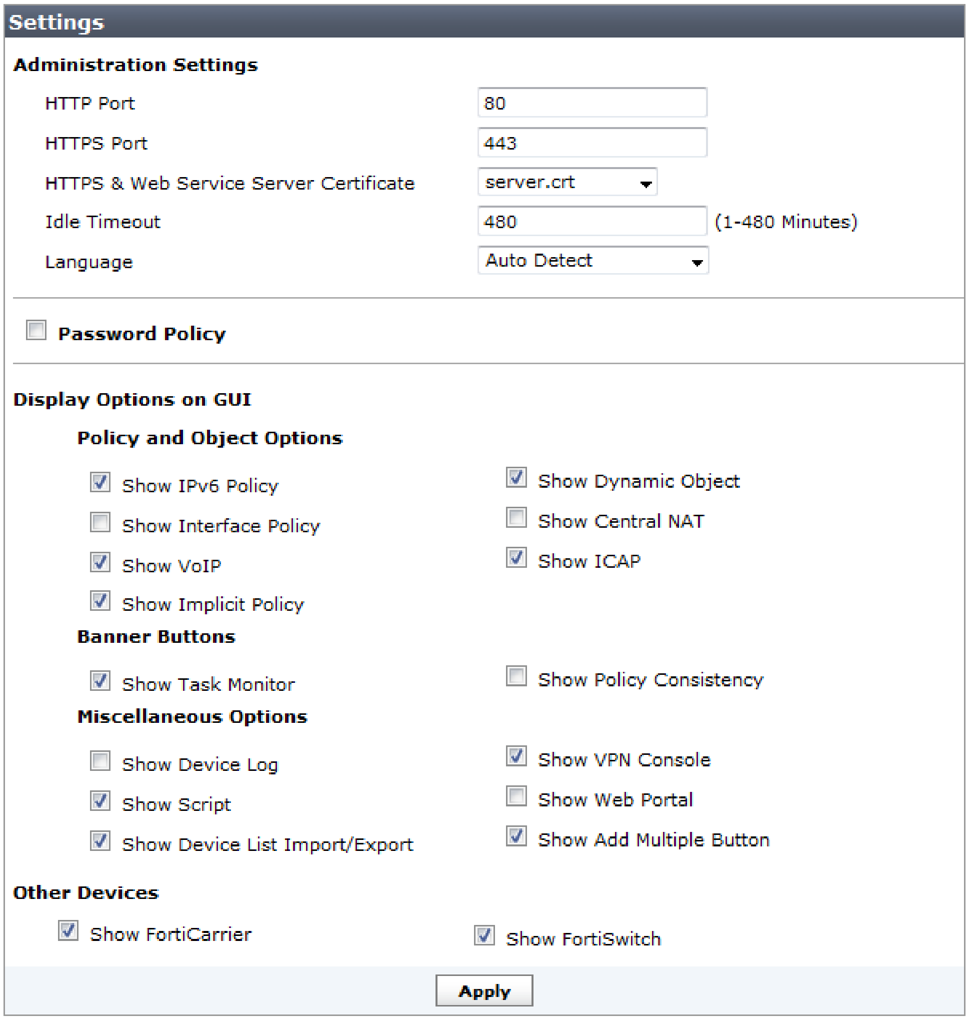
Only the `admin` administrator can configure these system options, which apply to all administrators logging onto the FortiManager unit.

To configure the administrative settings:

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

   The *Settings* window opens.

Figure 51: Administrative settings dialog box



Settings

Administration Settings

HTTP Port: 80

HTTPS Port: 443

HTTPS & Web Service Server Certificate: server.crt

Idle Timeout: 480 (1-480 Minutes)

Language: Auto Detect

□ Password Policy

Display Options on GUI

Policy and Object Options

☑ Show IPv6 Policy
☐ Show Interface Policy
☑ Show VoIP
☑ Show Implicit Policy
☑ Show Dynamic Object
☐ Show Central NAT
☑ Show ICAP

Banner Buttons

☑ Show Task Monitor
☐ Show Policy Consistency

Miscellaneous Options

☐ Show Device Log
☑ Show Script
☑ Show Device List Import/Export
☑ Show VPN Console
☐ Show Web Portal
☑ Show Add Multiple Button

Other Devices

☑ Show FortiCarrier
☑ Show FortiSwitch

2. Configure the following information:

Administration Settings	
HTTP Port	Enter the TCP port to be used for administrative HTTP access.
HTTPS Port	Enter the TCP port to be used for administrative HTTPS access.
HTTPS & Web Service Server Certificate	Select a certificate from the drop-down list.

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.
Language	Select a language from the drop-down list.
Password Policy	Select to enable administrator passwords.
Minimum Length	Select the minimum length for a password. The default is eight characters.
Must Contain	Select the types of characters that a password must contain.
Admin Password Expires after	Select the number of days that a password is valid for, after which time it must be changed.
Display Option on GUI	
Global Level	Select whether or not Global Policy Settings and Global Object Settings are shown.
ADOM Level	
Policy and Object Options	Select the required options from the list.
Banner Buttons	Select the required options from the list.
Miscellaneous Options	Select the required options from the list.
Other Devices	Select whether other device settings are shown.

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

Advanced

The *System Settings* > *Advanced* menu enables you to configure SNMP, meta field data, and other settings. The following options are available:

SNMP v1/v2c	Select to configure FortiGate and FortiManager reporting through SNMP traps. See “SNMP v1/v2c” on page 93.
Meta Fields	Select to configure metadata fields for FortiGate objects, and for FortiGate-5000 series shelf managers. See “Meta fields” on page 100
Advanced settings	Select to configure global advanced settings such as offline mode, device synchronization settings and install interface policy only; see “Advanced settings” on page 103.

Alerts	Select to configure alert events, mail and syslog servers, and to view alert messages. See “Alerts” on page 105
Device Log	Select to configure log settings and access and to view the task monitor. See “Device Log” on page 111

SNMP v1/v2c

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 > Advanced > 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 “RTM Profiles” on page 228.

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.

This section deals only with FortiManager system generated SNMP traps, not FortiGate unit generated traps. For information on FortiGate unit generated traps, see “RTM Profiles” on page 228.

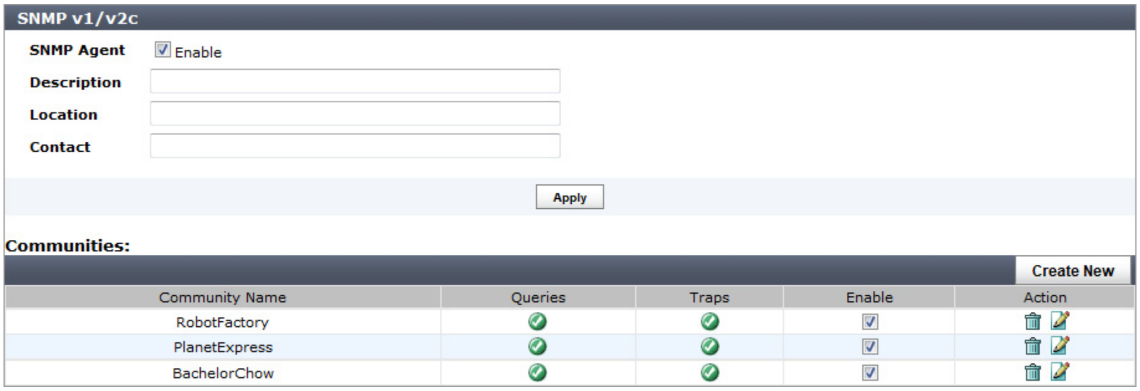
Configuring the SNMP agent

The SNMP agent sends SNMP traps that originate on the FortiManager system to an external monitoring SNMP manager defined in one of the FortiManager SNMP communities. Typically an SNMP manager is an application on a local computer that can read the SNMP traps and generate reports or graphs from them.

The SNMP manager can monitor the FortiManager system to determine if it is operating properly, or if there are any critical events occurring. The description, location, and contact information for this FortiManager system will be part of the information an SNMP manager will have — this information is useful if the SNMP manager is monitoring many devices, and it will enable faster responses when the FortiManager system requires attention.

Go to *System Settings > Advanced > SNMP v1/v2c* to configure the SNMP agent.

Figure 52:SNMP configuration



SNMP v1/v2c

SNMP Agent ☑ Enable

Description

Location

Contact

Apply

Communities:

Create New

Community Name	Queries	Traps	Enable	Action
RobotFactory	✓	✓	☑	🗑 ✎
PlanetExpress	✓	✓	☑	🗑 ✎
BachelorChow	✓	✓	☑	🗑 ✎

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.
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 95.
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.

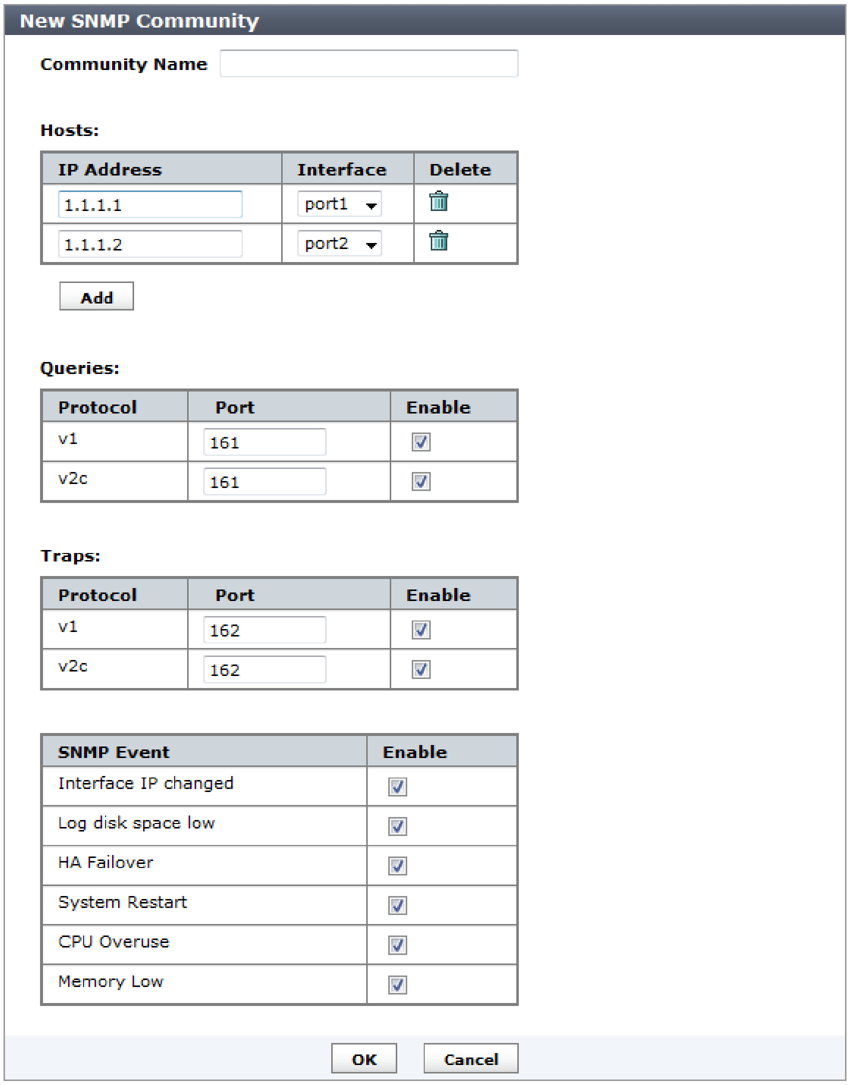
These SNMP communities do not refer to the FortiGate devices the FortiManager system is managing. For more information on FortiGate device SNMP, see either "RTM Profiles" on page 228, or the *FortiGate Administration Guide*.

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

Select *Create New* on the SNMP v1/v2c screen to open the *New SNMP Community* dialog box, where you can configure a new SNMP community. See Table 53 on page 96.

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 53: FortiManager SNMP Community



New SNMP Community

Community Name

Hosts:

IP Address	Interface	Delete
1.1.1.1	port1	🗑
1.1.1.2	port2	🗑

Queries:

Protocol	Port	Enable
v1	161	☑
v2c	161	☑

Traps:

Protocol	Port	Enable
v1	162	☑
v2c	162	☑

SNMP Event	Enable
Interface IP changed	☑
Log disk space low	☑
HA Failover	☑
System Restart	☑
CPU Overuse	☑
Memory Low	☑

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 from the drop-down list. 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 entry.
Add	Select to add a new default entry to the Hosts list that you can edit as needed. You can have up to eight SNMP manager entries for a single community.

Queries	Enter the port numbers (161 by default) that the FortiManager system uses to send SNMP v1 and SNMP v2c queries to the FortiManager in this community. Enable queries for each SNMP version that the FortiManager system uses.
Traps	Enter the Remote port numbers (162 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 • CPU Overusage • Memory Low

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 Customer Service & Support. To be able to communicate with the SNMP agent, you must compile all of these MIBs into your SNMP manager. Generally your SNMP manager will be an application on your local computer.

Your SNMP manager might already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet and FortiManager proprietary MIBs to this database.

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 98 and “Fortinet & FortiManager MIB fields” on page 99.
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 99.

Table 2: Fortinet MIBs (continued)

MIB file name or RFC	Description
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.

Table 4: Fortinet system traps (continued)

Trap message	Description
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.
fmTrapHASwitch	The FortiManager HA cluster has been re-arranged. A new master has been selected and asserted.

Meta fields

The *System Settings* > *Advanced* > *Meta Fields* menu 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.

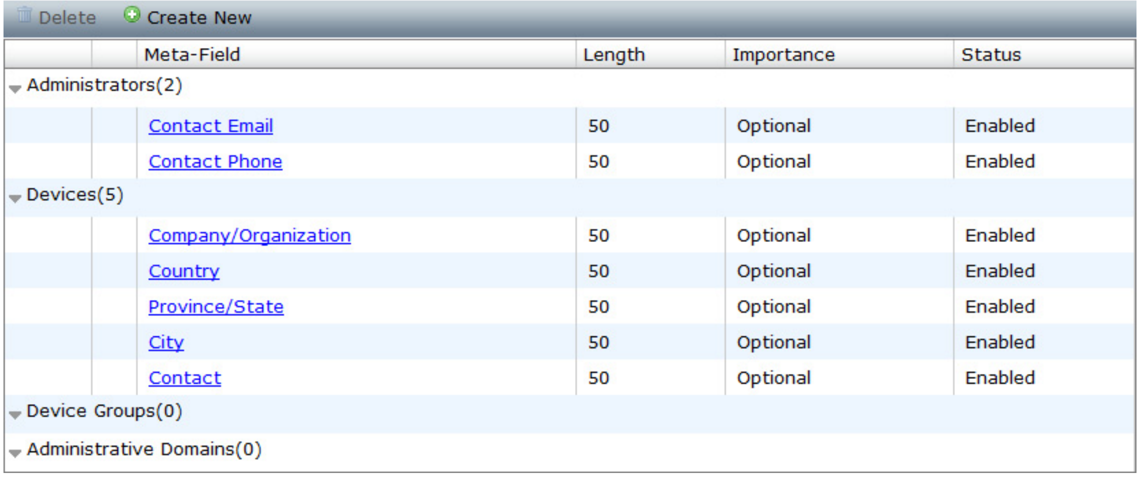
With the fields set as mandatory, administrators must supply additional information when they create a new FortiGate object, such as an administrator account or firewall policy. Fields for this new information are added to the FortiGate unit dialog boxes in the locations where you create these objects. You can also provide fields for optional additional information.

The one exception to this is the Administrators system object. This object applies only to administrators on the FortiManager unit. All other objects are related to FortiGate units.

System objects meta

Go to *System Settings* > *Advanced* > *Meta Fields* > *System Objects Meta* to add metadata fields for system-wide objects. The list of system object metadata fields appears; see Figure 54.

Figure 54: System objects metadata



Meta-Field	Length	Importance	Status
Administrators(2)			
Contact Email	50	Optional	Enabled
Contact Phone	50	Optional	Enabled
Devices(5)			
Company/Organization	50	Optional	Enabled
Country	50	Optional	Enabled
Province/State	50	Optional	Enabled
City	50	Optional	Enabled
Contact	50	Optional	Enabled
Device Groups(0)			
Administrative Domains(0)			

The following information is available:

Create New	Create a new metadata field for this object.
Delete	Select to delete this metadata field.
Meta-Field	The name of this metadata field. Select the name to edit this field.
Length	The maximum length of this metadata field.

Importance	Indicates whether this field is required or optional.
Status	Indicates whether this field is enabled or disabled.

To add a new metadata field:

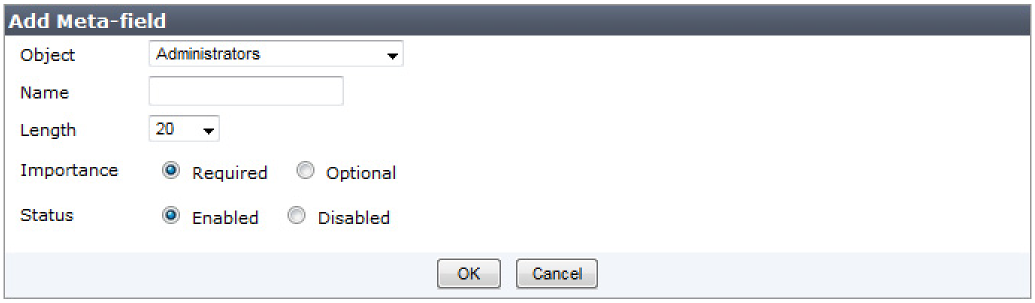
1. Go to *System Settings* > *Advanced* > *Meta Fields* > *System Objects Meta.*

   The list of configured system meta data objects appears; see Figure 54.

2. Select *Create New*.

   The *Add Meta-field* dialog box opens.

   Figure 55: Add a meta field



Object	Administrators
Name	
Length	20
Importance	● Required ○ Optional
Status	● Enabled ○ Disabled

3. Configure the following settings:

Object	The system 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 from the drop-down list (20, 50, or 255).
Importance	Select *Required* to make the field compulsory, otherwise select *Optional.*
Status	Select *Disabled* to disable this field. The default is enabled.

4. Select *OK* to save the new field.

To edit a metadata field:

1. Go to *System Settings* > *Advanced* > *Meta Fields* > *System Objects Meta.* The list of configured system meta data objects appears; see Figure 54.
2. Select the name of the meta field that you would like to edit to open the *Edit Meta-field* dialog box.

   Only the length, importance, and status of the meta field can be edited.

3. Edit the settings as required, and then select *OK* to apply the changes.

To delete metadata fields:

1. Go to *System Settings* > *Advanced* > *Meta Fields* > *System Objects Meta*.
2. Select meta fields that you would like to delete.

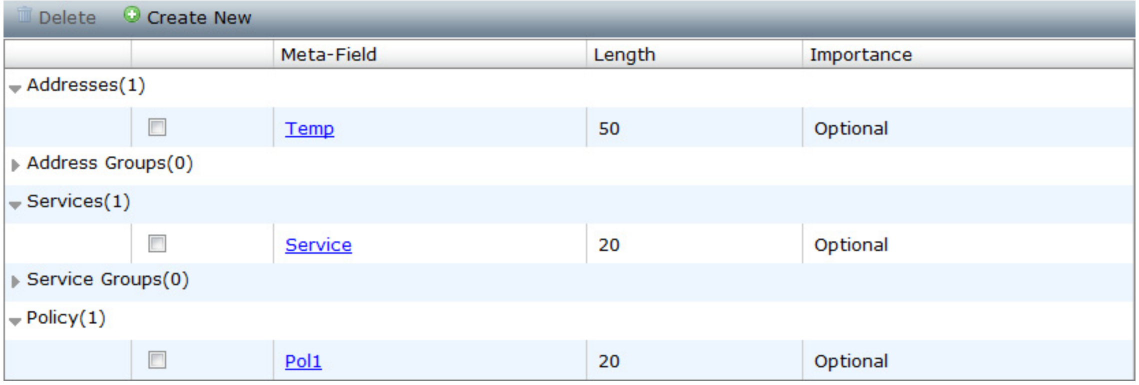
   The default meta fields cannot be deleted.

3. Select the *Delete* icon in the toolbar, then select *OK* in the confirmation box to delete the fields.

Config objects meta

Go to *System Settings* > *Advanced* > *Meta Fields* > *Config Objects Meta* to add metadata fields for FortiGate objects. The list of config object metadata fields appears; see Figure 56.

Figure 56: Config objects metadata



		Meta-Field	Length	Importance
Addresses(1)				
	□	Temp	50	Optional
Address Groups(0)				
Services(1)				
	□	Service	20	Optional
Service Groups(0)				
Policy(1)				
	□	Pol1	20	Optional

The following information is available:

Create New	Create a new metadata field for this object.
Delete	Select to delete this metadata field.
Meta-Field	The name of this metadata field. Select the name to edit this metadata field.
Length	The maximum length of this metadata field.
Importance	Indicates whether this field is required or optional.

To add a new config object metadata field:

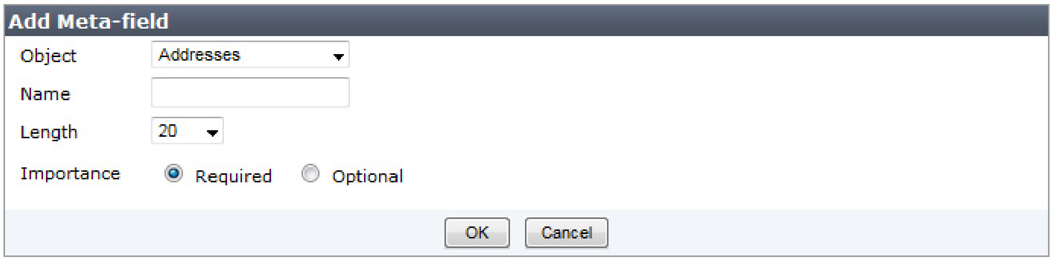
1. Go to *System Settings* > *Advanced* > *Meta Fields* > *Config Objects Meta.*

   The list of config object meta fields appears.

2. Select *Create New*.

   The *Add Meta-field* dialog box appears.

   Figure 57: Add meta field (config object)

   Add Meta-field

   Object: Addresses

   Name:

   Length: 20

   Importance: ● Required ○ Optional

3. Configure the following settings:

Object	The system 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 from the drop-down list (20, 50, or 255).
Importance	Select *Required* to make the field compulsory, otherwise select *Optional.*

4. Select *OK* to save the new field.

To edit a metadata field:

1. Go to *System Settings* > *Advanced* > *Meta Fields* > *Config Objects Meta.*

   The list of config object meta fields appears.

2. Select the name of the meta field that you would like to edit to open the *Edit Meta-field* dialog box.

   Only the length and importance of the meta field can be edited.

3. Edit the settings as required, and then select *OK* to apply the changes.

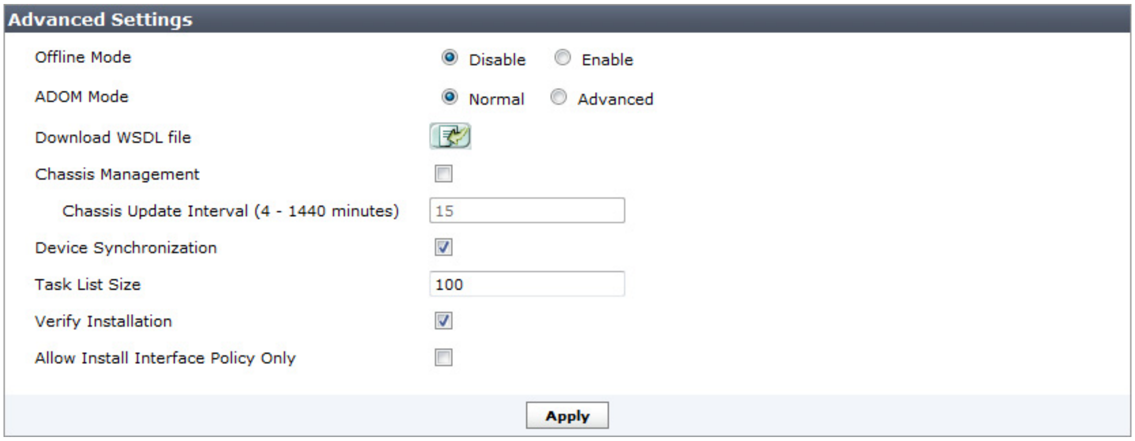
To delete metadata fields:

1. Go to *System Settings* > *Advanced* > *Meta Fields* > *Config Objects Meta*.
2. Select meta fields that you would like to delete.
3. Select the *Delete* icon in the toolbar, then select *OK* in the confirmation box to delete the fields.

Advanced settings

To view and configure advanced settings options, go to the *System Settings* > *Advanced* > *Advanced Settings* page. The *Advanced Settings* dialog box appears; see Figure 58.

Figure 58: Advanced settings



Advanced Settings

Offline Mode	● Disable ○ Enable
ADOM Mode	● Normal ○ Advanced
Download WSDL file	
Chassis Management	□
Chassis Update Interval (4 - 1440 minutes)	15
Device Synchronization	☑
Task List Size	100
Verify Installation	☑
Allow Install Interface Policy Only	□

Configure the following settings and then select *Apply*:

Offline Mode	Enabling *Offline Mode* shuts down the protocol used to communicate with managed devices. This is a feature you can use to troubleshoot problems, allowing you to change FortiManager unit settings without affect managed devices.
ADOM Mode	Select the ADOM mode, either *Normal* or *Advanced*.
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	Enable chassis management.
Chassis Update Interval	Enter a chassis update interval from 14 to 1440 minutes (default is 15). This option is only available if chassis management is enabled.
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.
Verify Installation	Select to preview the installation before proceeding.
Allow Install Interface Policy Only	Select to manage and install interface based policies only instead of all device and policy configuration.

Alerts

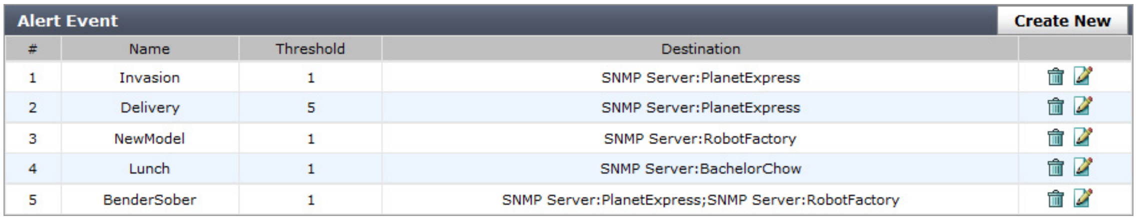
Alerts allow you to monitor and receive notification on specific activity on your network.

Alerts event

You can configure alert events by severity level and set thresholds. When an alert event occurs you can configure to have the alert event sent to an email address, SNMP server, or a syslog server.

To view the currently configured alert events, go to *System Settings* > *Advanced* > *Alerts* > *Alert Events*.

Figure 59: Alert event window



Alert Event — Create New

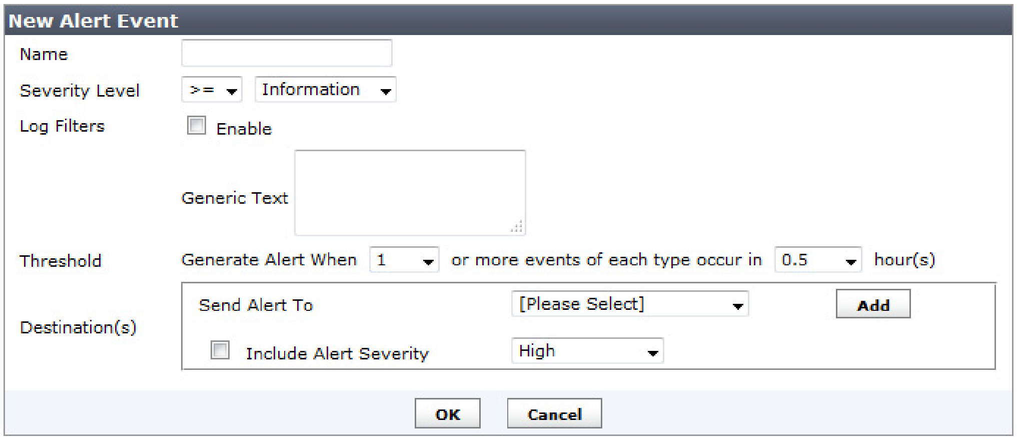
#	Name	Threshold	Destination
1	Invasion	1	SNMP Server:PlanetExpress
2	Delivery	5	SNMP Server:PlanetExpress
3	NewModel	1	SNMP Server:RobotFactory
4	Lunch	1	SNMP Server:BachelorChow
5	BenderSober	1	SNMP Server:PlanetExpress;SNMP Server:RobotFactory

To create a new alert event:

1. Go to *System Settings* > *Advanced* > *Alerts* > *Alert Events*.
2. Select the *Create New* toolbar icon.

   The *New Alert Event* window opens.

   Figure 60: Create new alert event

   New Alert Event

   Name

   Severity Level: >= Information

   Log Filters: □ Enable

   Generic Text

   Threshold: Generate Alert When 1 or more events of each type occur in 0.5 hour(s)

   Destination(s): Send Alert To [Please Select] Add

   □ Include Alert Severity High

   OK Cancel

3. Configure the following settings and then select *OK*:

Name	Enter a name for the alert event.
Severity Level	
Condition	Select the conditional value from the drop-down list: • Greater than or equal to: >= • Equal to: = • Less than or equal to: <=

Level	Select the severity level from the drop-down list: • Information • Notification • Warning • Error • Critical • Alert • Emergency
Log Filters	
Enable	Select to enable log filters.
Generic Text	Optional text field.
Threshold	
Generate Alert When	Generate an alert after: • 1 • 5 • 10 • 50 • 100 or more events of each type occurs.
Occurrence	Select from the drop-down list: • 0.5 • 1.0 • 3.0 • 6.0 • 12.0 • 24.0 • 168.0 hours.
Destination	
Send Alert To	Select a destination from the drop-down list, or select *[Create New...]* to create a new destination of the requisite type. The available destination types are: • Email Address • SNMP Server • Syslog Server
Add	Select to add the destination, or to add additional destinations. At least one destination must be added.

Include Alert Severity	Select to include alert severity level.
Level	Select the level to include from the drop-down list: • High • Medium High • Medium • Medium Low • Low

To edit an alert event:

1. Go to *System Settings* > *Advanced* > *Alerts* > *Alert Events.*
2. Select the *Edit* icon on the far right side of the alert's row that you would like to edit.

   The *Edit Alert Event* window opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

To delete an alert event:

1. Go to *System Settings* > *Advanced* > *Alerts* > *Alert Events.*
2. Select the *Delete* icon in the row of the alert event that you would like to delete.
3. Select *OK* in the confirmation box to delete the alert event.

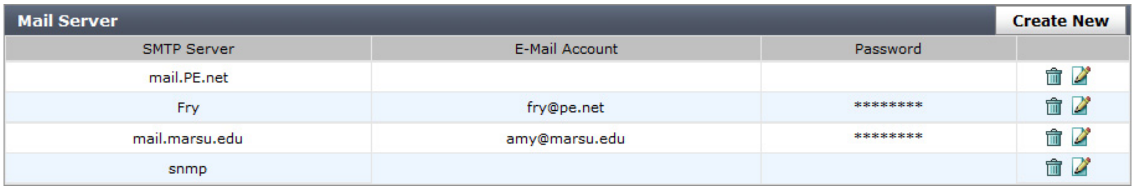
Mail server

Configure mail server settings for alerts, edit existing settings, or delete mail servers.

If an existing mail server is set in an Alerts Event configuration, the delete icon is removed and the mail server entry can not be deleted.

To view and configure mail servers, go to *System Settings* > *Advanced* > *Alerts* > *Mail Server*.

Figure 61: Mail server window



Mail Server

Create New

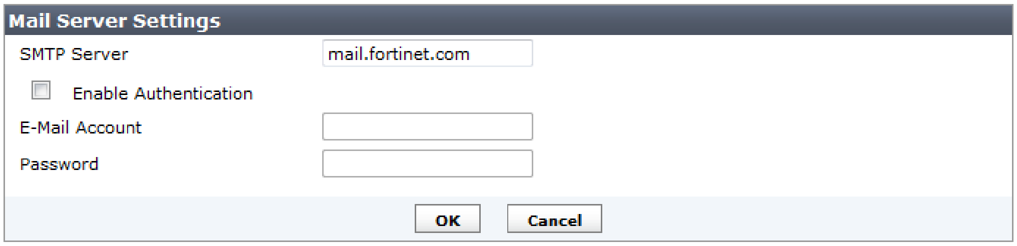
SMTP Server	E-Mail Account	Password	
mail.PE.net			🗑 ✎
Fry	fry@pe.net	********	🗑 ✎
mail.marsu.edu	amy@marsu.edu	********	🗑 ✎
snmp			🗑 ✎

To create a new mail server:

1. Go to *System Settings* > *Advanced* > *Alerts* > *Mail Server*.
2. Select *Create New*.

   The *Mail Server Settings* window opens.

Figure 62: Mail server settings



Mail Server Settings

SMTP Server	mail.fortinet.com
□ Enable Authentication	
E-Mail Account	
Password	

OK Cancel

3. Configure the following settings and then select *OK*:

SMTP Server	Enter the SMTP server domain information, e.g. mail@company.com.
Enable Authentication	Select to enable authentication.
Email Account	Enter an email account, e.g. admin@company.com.
Password	Enter the email account password.

To edit a mail server:

1. Go to *System Settings* > *Advanced* > *Alerts* > *Mail Server*.
2. Select the *Edit* icon on the far right side of the server's row that you would like to edit.

   The *Mail Server Settings* window opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

To delete a mail server:

1. Go to *System Settings* > *Advanced* > *Alerts* > *Mail Server*.
2. Select the *Delete* icon in the row of the mail server that you would like to delete.
3. Select *OK* in the confirmation box to delete the server.

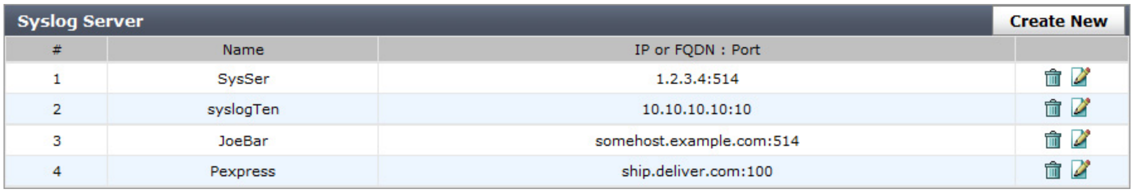
Syslog Server

Configure syslog server settings for alerts, edit existing settings, or delete syslog servers.

If an existing syslog server is set in an Alerts Event configuration, the delete icon is removed and the syslog server entry can not be deleted.

To view and configure syslog servers, go to *System Settings* > *Advanced* > *Alerts* > *Syslog Server*.

Figure 63: Syslog server window



Syslog Server Create New

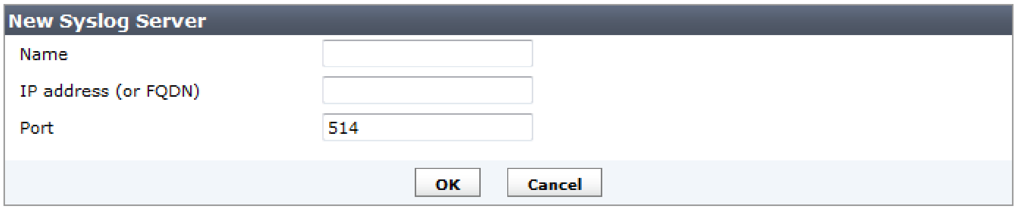
#	Name	IP or FQDN : Port	
1	SysSer	1.2.3.4:514	
2	syslogTen	10.10.10.10:10	
3	JoeBar	somehost.example.com:514	
4	Pexpress	ship.deliver.com:100	

To create a new syslog server:

1. Go to *System Settings* > *Advanced* > *Alerts* > *Syslog Server*.
2. Select *Create New*.

   The *New Syslog Server* window opens.

   Figure 64: Syslog server settings

   New Syslog Server

   Name

   IP address (or FQDN)

   Port 514

3. Configure the following settings and then select *OK*:

Name	Enter a name for the syslog server.
IP address (or FQDN)	Enter the IP address or FQDN of the syslog server.
Port	Enter the syslog server port number. The default value is 514.

To edit a syslog server:

1. Go to *System Settings* > *Advanced* > *Alerts* > *Syslog Server*.
2. Select the *Edit* icon on the far right side of the server’s row that you would like to edit.

   The *Edit Syslog Server* window opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

To delete a syslog server:

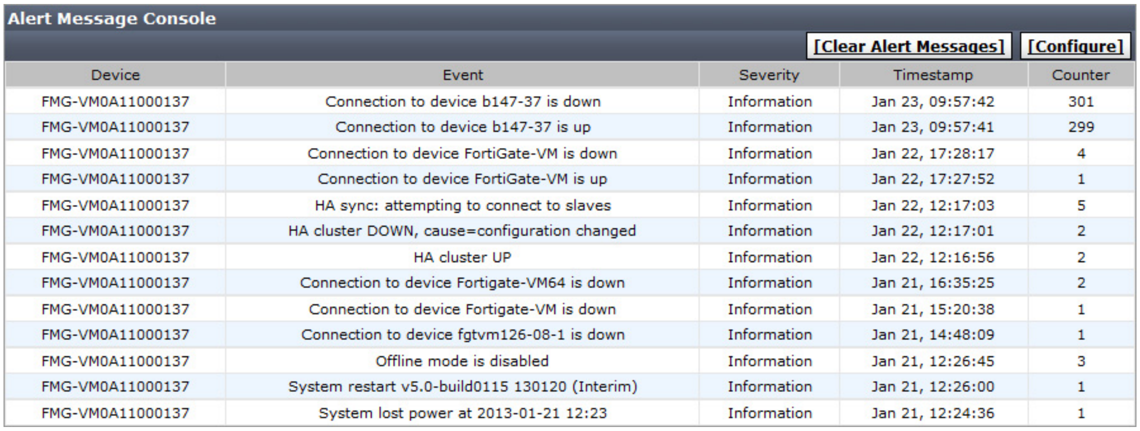
1. Go to *System Settings* > *Advanced* > *Alerts* > *Syslog Server*.
2. Select the *Delete* icon in the row of the server that you would like to delete.
3. Select *OK* in the confirmation box to delete the server.

Alert Console

The Alert Console allows you to view alert events based on specific time frames or severity levels. It also allows you to clear all previous alert events.

To view the Alert Console, go to *System Settings* > *Advanced* > *Alerts* > *Alert Console*.

Figure 65: Alert message console window



Alert Message Console

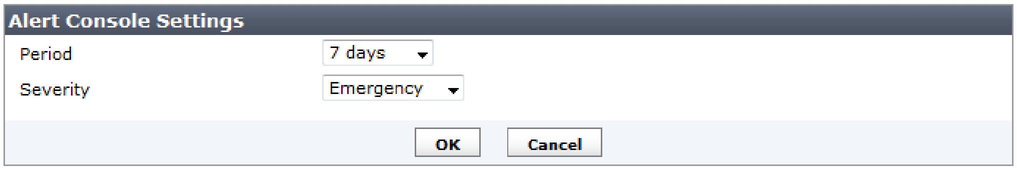
Device	Event	Severity	Timestamp	Counter
FMG-VM0A11000137	Connection to device b147-37 is down	Information	Jan 23, 09:57:42	301
FMG-VM0A11000137	Connection to device b147-37 is up	Information	Jan 23, 09:57:41	299
FMG-VM0A11000137	Connection to device FortiGate-VM is down	Information	Jan 22, 17:28:17	4
FMG-VM0A11000137	Connection to device FortiGate-VM is up	Information	Jan 22, 17:27:52	1
FMG-VM0A11000137	HA sync: attempting to connect to slaves	Information	Jan 22, 12:17:03	5
FMG-VM0A11000137	HA cluster DOWN, cause=configuration changed	Information	Jan 22, 12:17:01	2
FMG-VM0A11000137	HA cluster UP	Information	Jan 22, 12:16:56	2
FMG-VM0A11000137	Connection to device Fortigate-VM64 is down	Information	Jan 21, 16:35:25	2
FMG-VM0A11000137	Connection to device Fortigate-VM is down	Information	Jan 21, 15:20:38	1
FMG-VM0A11000137	Connection to device fgtvm126-08-1 is down	Information	Jan 21, 14:48:09	1
FMG-VM0A11000137	Offline mode is disabled	Information	Jan 21, 12:26:45	3
FMG-VM0A11000137	System restart v5.0-build0115 130120 (Interim)	Information	Jan 21, 12:26:00	1
FMG-VM0A11000137	System lost power at 2013-01-21 12:23	Information	Jan 21, 12:24:36	1

To configure the alert console:

1. Go to *System Settings* > *Advanced* > *Alerts* > *Alert Console*.
2. Select *Configure*.

   The *Alert Console Settings* window opens.

   Figure 66: Alert console settings

   Alert Console Settings

   Period: 7 days

   Severity: Emergency

3. Configure the following settings and then select *OK*:

Period	Select the time period to display from the drop-down list, from one to seven days.
Severity	Select the alert severity level to display from the drop-down list. Options include: *Debug*, *Information, Notification, Warning*, *Error, Critical*, *Alert*, and *Emergency*.

To clear the alert console:

1. Go to *System Settings* > *Advanced* > *Alerts* > *Alert Console*.
2. Select *Clear Alert Messages*.
3. Select *OK* in the confirmation box to clear all the alert messages in the console.

Device Log

The FortiManager allows you to log system events to disk. For more information, see “Log View” on page 238.

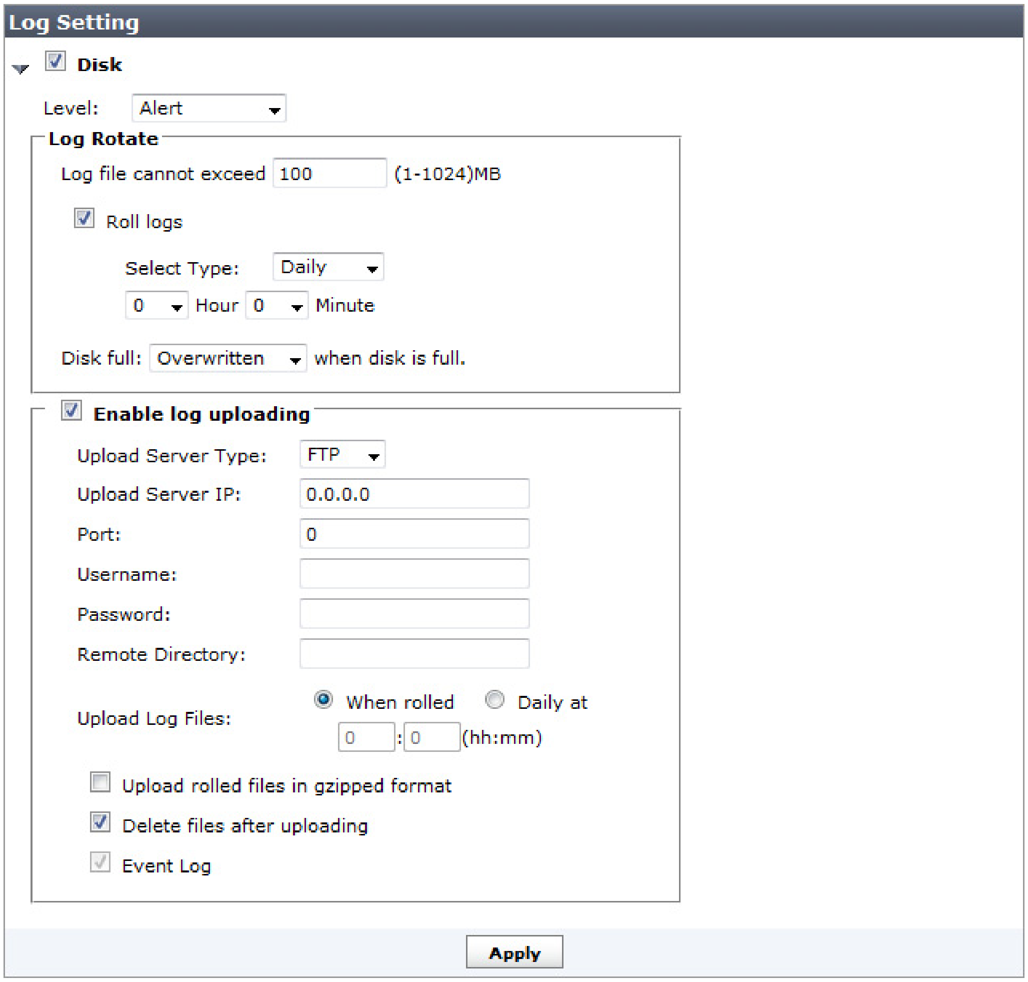
Log Setting

The log settings menu window allows you to configure event logging to disk, and allows you to configure the following options:

- Severity level of logged events
- Log rotation settings
- Log uploading

To configure log settings, go to *System Settings* > *Advanced* > *Device Log* > *Log Setting*,

Figure 67: Log setting window



Log Setting

☑ Disk

Level: Alert

Log Rotate

Log file cannot exceed 100 (1-1024)MB

☑ Roll logs

Select Type: Daily

0 Hour 0 Minute

Disk full: Overwritten when disk is full.

☑ Enable log uploading

Upload Server Type: FTP

Upload Server IP: 0.0.0.0

Port: 0

Username:

Password:

Remote Directory:

Upload Log Files: ● When rolled ○ Daily at

0 : 0 (hh:mm)

☐ Upload rolled files in gzipped format

☑ Delete files after uploading

☑ Event Log

Configure the following settings and then select *Apply*:

Disk	Select to enable log setting configuration.
Level	Select the level of the notification from the drop-down list. Options include: *Emergency*, *Alert, Critical*, *Error, Warning*, *Notification*, *Information*, and *Debug*.

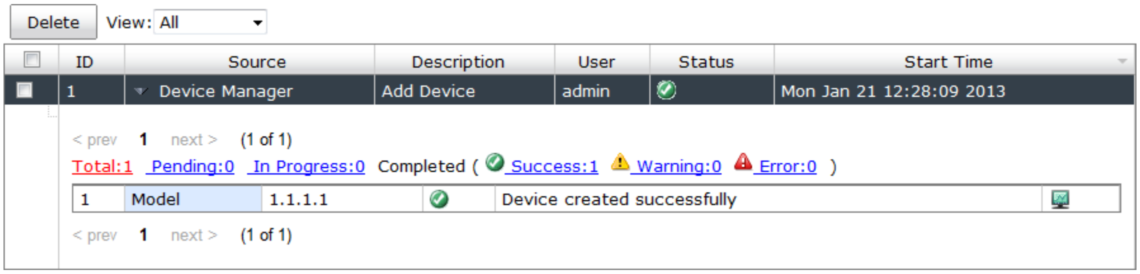
Log Rotate	
Log file cannot exceed	Enter the maximum log size in megabytes. Maximum allowed log file size is 1024MB.
Roll logs	Select to roll the logs.
Select Type	Select to roll the logs on a weekly or daily basis.
Select One Day	Select the day of the week to roll the logs. This option is enabled only when *Roll Logs* is selected and the *Type* is Weekly.
Time	Select the Hour and Minute of the day to roll the logs. The hour is based on a 24 hour clock.
Disk full	Select the action to take when the disk is full, either *Overwritten* or *Do not log*, from the drop-down list.
Enable log uploading	Select to upload realtime device logs.
Upload Server Type	Select one of *FTP*, *SFTP*, *SCP*, or *FAZ*.
Upload Server IP	Enter the IP address of the upload server.
Port	Enter the port 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.
Event Log	This option is not available.

Task Monitor

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

Go to *System Settings* > *Advanced* > *Device Log* > *Task Monitor*, then select a task category from the *View* field drop-down list, or leave as the default *All*.

Figure 68: Task monitor window



View: All

□	ID	Source	Description	User	Status	Start Time
□	1	Device Manager	Add Device	admin	✓	Mon Jan 21 12:28:09 2013

< prev 1 next > (1 of 1)

Total:1 Pending:0 In Progress:0 Completed (✓ Success:1 ⚠ Warning:0 ⚠ Error:0)

1	Model	1.1.1.1	✓	Device created successfully	

< prev 1 next > (1 of 1)

Delete	Remove the selected task or tasks from the list.
View	Select which tasks to view from the drop-down list, based on their status. The available options are: *Running*, *Pending*, *Done*, *Error*, *Cancelling*, *Cancelled*, *Aborting*, *Aborted*, *Warning*, and *All* (default).
ID	The identification number for a task.
Source	The platform from where the task is performed.
Expand Arrow	Select to display the specific actions taken under this task. To filter the specific actions taken for a task, select one of the options on top of the action list.
Description	The nature of the task.
User	The users who have performed the tasks.
Status	The status of the task (hover over the icon to view the description): • *All*: All types of tasks. • *Done*: Completed with success. • *Error*: Completed without success. • *Cancelled*: User cancelled the task. • *Cancelling*: User is cancelling the task. • *Aborted*: The FortiManager system stopped performing this task. • *Aborting*: The FortiManager system is stopping performing this task. • *Running*: Being processed. In this status, a percentage bar appears in the Status column.
Start Time	The time that the task was performed.

Device Manager

Use the *Device Manager* tab to view and configure managed devices. The *Device Manager* tab also provides access to scripts, and web portal features. For more information on script and web portal features, see “Advanced Features” on page 196.

This section focuses on improvements and changes to the *Device Manager* tab, navigating the *Device Manager* tab, viewing devices, and managing devices. For information on adding devices, and installing policy packages see “FortiManager Wizards” on page 158.

Additional configuration options and short-cuts are available using the right-click content menu. Right-click the mouse on different parts of the navigation panes on the Web-based Manager page to access these context menus.

Device Manager tab

FortiManager v5.0 introduces the following improvements and changes to the *Device Manager* tab:

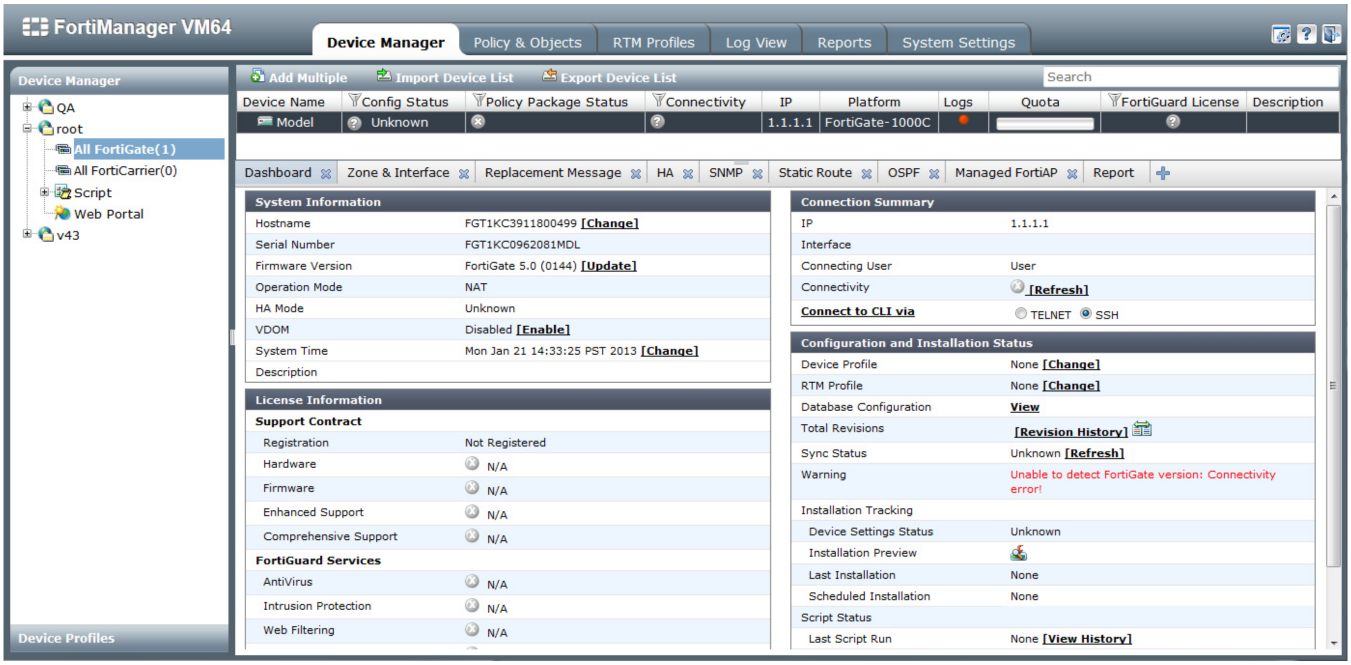
- Device Manager tab layout
- Device policy package status
- Device profiles
- Extend workspace to entire ADOM
- Quick install

Device Manager tab layout

The *Device Manager* tab now has collapsed ADOM navigation, where all of the ADOMs are displayed on the tree-menu; you do not need to enter each ADOM individually. The *Device Manager* tab has the following changes:

- The device groups, *All FortiGate, All FortiCarrier,* custom device groups, and device profiles are displayed under each ADOM.
- The number of devices is displayed in parentheses next to each device group name.
- Script and Web Portal features are disabled by default. You can enable these advanced configuration options under *System Systems* > *Admin* > *Admin Settings*. Select *Show Script*, and *Show Web Portal* to enable on these options on the *Device Manager* tab tree-menu.

Figure 69: Device Manager layout



Device Name	Config Status	Policy Package Status	Connectivity	IP	Platform	Logs	Quota	FortiGuard License	Description
Model	Unknown			1.1.1.1	FortiGate-1000C	●			

System Information	
Hostname	FGT1KC3911800499 [Change]
Serial Number	FGT1KC0962081MDL
Firmware Version	FortiGate 5.0 (0144) [Update]
Operation Mode	NAT
HA Mode	Unknown
VDOM	Disabled [Enable]
System Time	Mon Jan 21 14:33:25 PST 2013 [Change]
Description	

License Information	
Support Contract	
Registration	Not Registered
Hardware	N/A
Firmware	N/A
Enhanced Support	N/A
Comprehensive Support	N/A
FortiGuard Services	
AntiVirus	N/A
Intrusion Protection	N/A
Web Filtering	N/A

Connection Summary	
IP	1.1.1.1
Interface	
Connecting User	User
Connectivity	[Refresh]
Connect to CLI via	○ TELNET ● SSH

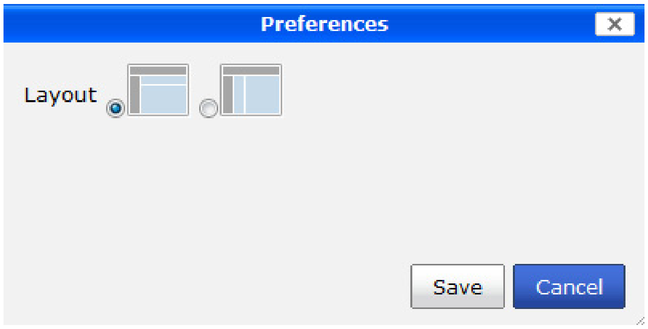
Configuration and Installation Status	
Device Profile	None [Change]
RTM Profile	None [Change]
Database Configuration	View
Total Revisions	[Revision History]
Sync Status	Unknown [Refresh]
Warning	Unable to detect FortiGate version: Connectivity error!
Installation Tracking	
Device Settings Status	Unknown
Installation Preview	
Last Installation	None
Scheduled Installation	None
Script Status	
Last Script Run	None [View History]

The *All FortiCarrier* device group is not enabled by default. To enable this device group, go to *System Systems > Admin > Admin Settings.* Select *Show FortiCarrier* to enable.

Add Multiple, Import Device List, and *Export Device List* are only available on the horizontal view.

The right pane has two possible views: Horizontal and Vertical. You can select the preferences button to change the view-mode between horizontal and vertical views.

Figure 70: Preferences button location and window



There is a quick filter option available in vertical view to quickly find devices in certain states including *Connection Down, Config Changed,* and *License Expired.* The Web-based Manager will remember the state of the quick filter when returning to the *Device Manager* tab. Filters in Horizontal view are set per column.

Horizontal view

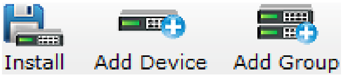
In the horizontal view, the top portion of the right content pane shows the device list. When you select one of the devices in the table, the bottom portion of the right content pane displays the selected device dashboard. The menu navigation of the device settings is changed to a tab format, the dashboard toolbar, see Figure 69 on page 115.

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

If ADOMs are enabled, the navigation pane *Install*, *Add device*, and *Add Group* icons are hidden. You can use the right-click context menus within an ADOM to launch the *Add Device* and *Install* wizards, and perform other menu actions including creating device groups.

If ADOMs are not enabled then the top level navigation pane with icons is visible.

Figure 71: Device manager toolbar buttons

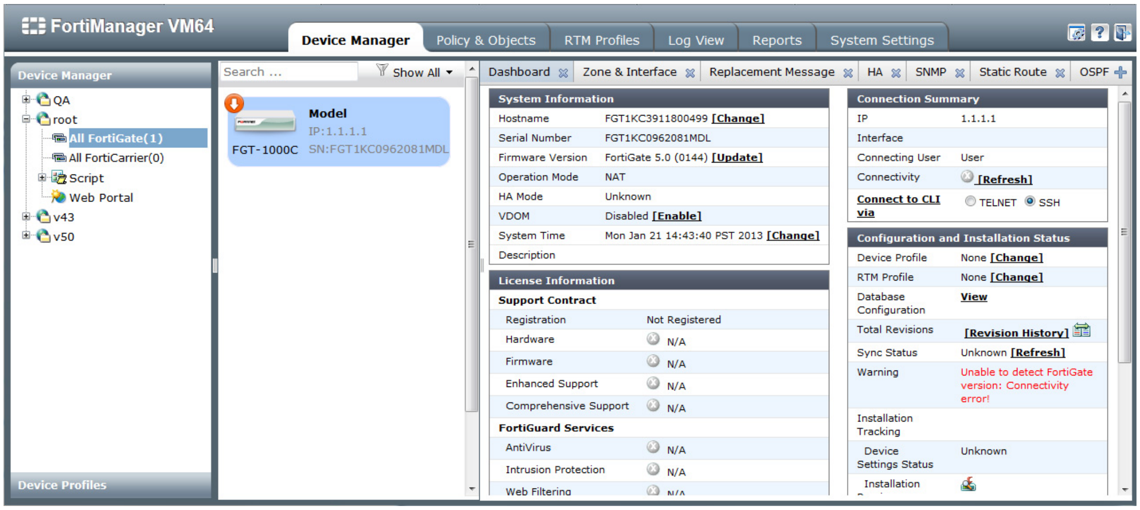


If the administrator hovers their cursor over an ADOM, information will be displayed about that ADOM including the ADOM version, Mode, and VPN management options.

Vertical view

The vertical view is similar to the horizontal view, except that the devices are displayed on a vertical list on the left side of the content frame. Vertical view offers a simplified view of the *Device Manager* tab.

Figure 72: Device manager vertical view example



Model
IP:1.1.1.1
FGT-1000C SN:FGT1KC0962081MDL

System Information	
Hostname	FGT1KC3911800499 [Change]
Serial Number	FGT1KC0962081MDL
Firmware Version	FortiGate 5.0 (0144) [Update]
Operation Mode	NAT
HA Mode	Unknown
VDOM	Disabled [Enable]
System Time	Mon Jan 21 14:43:40 PST 2013 [Change]
Description	

License Information	
Support Contract	
Registration	Not Registered
Hardware	N/A
Firmware	N/A
Enhanced Support	N/A
Comprehensive Support	N/A
FortiGuard Services	
AntiVirus	N/A
Intrusion Protection	N/A
Web Filtering	N/A

Connection Summary	
IP	1.1.1.1
Interface	
Connecting User	User
Connectivity	[Refresh]
Connect to CLI via	○ TELNET ● SSH

Configuration and Installation Status	
Device Profile	None [Change]
RTM Profile	None [Change]
Database Configuration	View
Total Revisions	[Revision History]
Sync Status	Unknown [Refresh]
Warning	Unable to detect FortiGate version: Connectivity error!
Installation Tracking	
Device Settings Status	Unknown
Installation	

Add Multiple, *Import Device List*, and *Export Device List* are only available on the horizontal view.

Vertical view does not have the column settings found in horizontal view. When you hover the mouse cursor over the device/VDOM, a pop-up window is displayed with the following information: device type, firmware version, connectivity, HA mode, FortiGuard license, and configuration status.

Device dashboard

An icon has been added to the *Configuration and Installation Status* widget for when a device is synchronized, but the configuration was retrieved from the device (e.g. modifications were made directly on the FortiGate and synchronized to the FortiManager). A tool tip will show the last date and time that the sync occurred.

The widgets have changed as follows:

- The Unit Operation widget has been removed.
- The System Information widget has the following changes:
  - Add *[Change]* to HA Mode and launch HA dialog
  - Remove *Session Information* field
- The License Information widget has been updated.

Device policy package status

To view policy configuration status, right-click in the content pane, select *Column Settings*, then *Policy Package Status*. When you hover the mouse cursor over the column icon, you can see when the last check was performed. When the admin makes a change to any policies, the corresponding policy package will be deemed *dirty*, and will show as such in the device list.

On *Column Settings*, you can choose to display the following information:

Config Status	Platform	Logs	Description
Connectivity	FortiGuard License	Quota	Contact
IP	Policy Package Status	Firmware Version	Log Connection
City	Province	Country	Company

Column settings only apply to the horizontal view. The vertical view has a quick filter option next to the search window where you can select *View All, Connection Down, Config Changed,* and *License Expired*.

Device profiles

A device profile is a subset of a model device configuration. Each device or device group can be linked with a device profile. When linked, the selected settings will come from the profile, not from the *Device Manager* database.

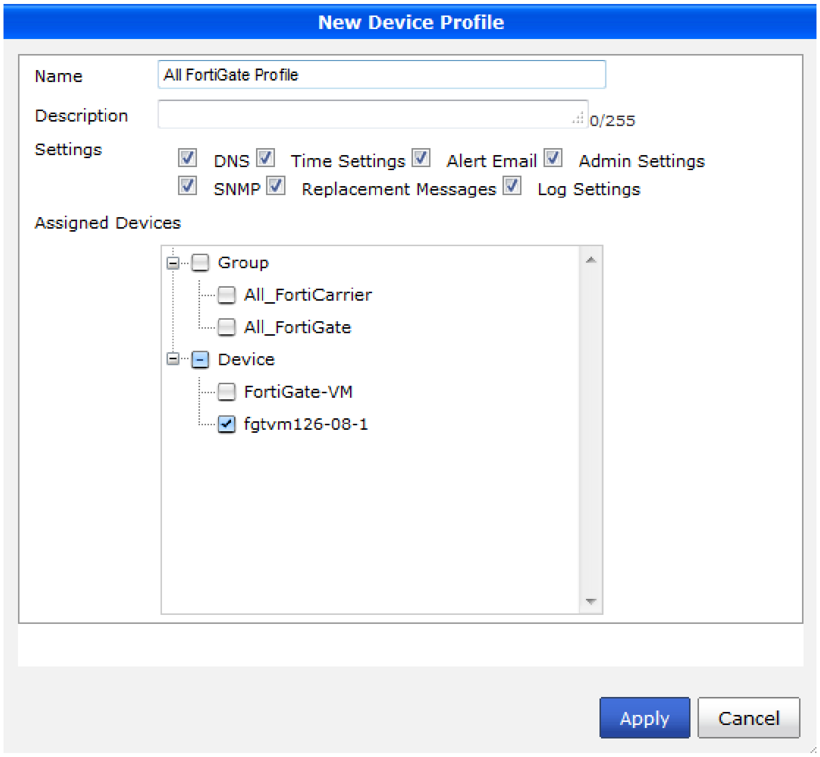
By default, there is one generic profile defined. Device profiles are managed in a similar manner to policy packages. You can use the context menus to create new device profiles.

Device profiles will support the following settings:

- DNS: Networking options including DNS settings and local domain name.
- Time settings (NTP server settings)
- Alert Email
- Admin settings: Configuration options including central management, web administration ports, timeout settings, and web administration.
- SNMP
- Replacement messages (Global only, you can customize per VDOM replacement messages)
- Log settings: Logging and archiving settings to configure logging to a FortiAnalyzer/FortiManager or a syslog server.

You can create or delete profiles with a context menu by right-clicking the profile. You can then select particular devices that will be associated with the profile. You can link a device to the device profile using the *Add Device Wizard*, from the device's dashboard page in *Device Manager*, or by right-clicking to edit the profile and select devices.

Figure 73: New device profile



New Device Profile

Name: All FortiGate Profile

Description: 0/255

Settings: ☑ DNS ☑ Time Settings ☑ Alert Email ☑ Admin Settings ☑ SNMP ☑ Replacement Messages ☑ Log Settings

Assigned Devices:

- □ Group
  - □ All_FortiCarrier
  - □ All_FortiGate
- ⊟ Device
  - □ FortiGate-VM
  - ☑ fgtvm126-08-1

Extend workspace to entire ADOM

When concurrent ADOM access is enabled, administrators are able to lock the ADOM. A right-click menu option has been added to allow you to lock/unlock ADOM access. The ADOM lock status is displayed by a lock icon to the left of the ADOM name. The lock status is as follows:

- Grey lock: The ADOM is currently unlocked, and is read/write.
- Green lock: The ADOM is locked by you when logged in as an admin.
- Red lock: The ADOM is locked by another admin.

To enable and disable workspaces:

1. Select the *System Settings* tab on the navigation pane.
2. Go to *System Settings* > *General* > *Dashboard*.
3. In the CLI Console widget enter the following CLI command:

```
config system global
  set workspace enable | disable
end
```

4. The FortiManager session will end and you must log back into the FortiManager system.

Workspace is disabled by default. When workspace is enabled, the *Device Manager* tab and *Policy & Objects* tab are read-only. You must lock the ADOM to enable read-write access to make changes to the ADOM.

An additional CLI command has been added to enable or disable ADOM lock override:

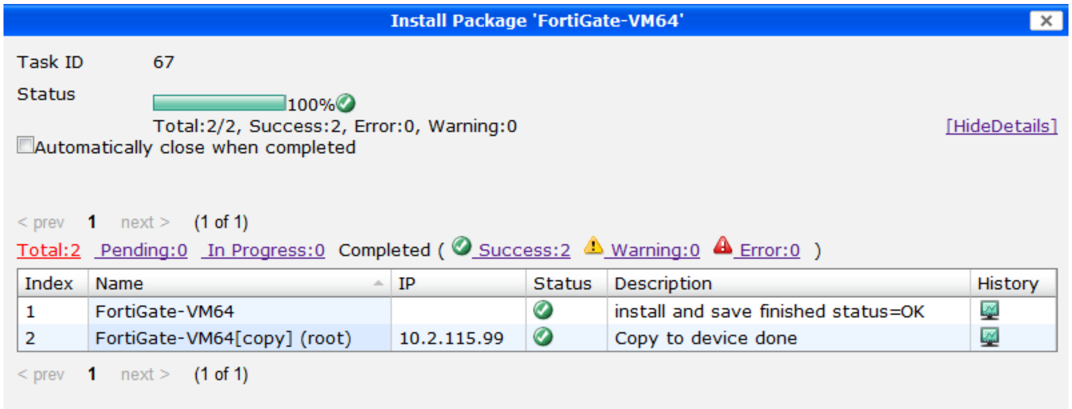
```
config system global
  set lock-preempt [enable | disable]
```

When the ADOM lock override is enabled, if two administrators are concurrently accessing an ADOM and one attempts to lock the ADOM, the other admin can kick the admin off the ADOM, preventing the ADOM from being locked.

Quick install

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

Figure 74: Quick install without launching wizard



Install Package 'FortiGate-VM64'

Task ID 67

Status 100% ✓

Total:2/2, Success:2, Error:0, Warning:0

[HideDetails]

☐ Automatically close when completed

< prev 1 next > (1 of 1)

Total:2 Pending:0 In Progress:0 Completed (✓ Success:2 ⚠ Warning:0 ⚠ Error:0)

Index	Name	IP	Status	Description	History
1	FortiGate-VM64		✓	install and save finished status=OK	🖥
2	FortiGate-VM64[copy] (root)	10.2.115.99	✓	Copy to device done	🖥

< prev 1 next > (1 of 1)

Viewing managed device

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

This section contains the following topics:

- Using column filters
- View managed devices
- Dashboard widgets

Using column filters

You can filter each column, by selecting the column header. Use the right-click menu to access the context menu to add or remove columns.

The following table describes the available columns and filters available per column.

Table 10: Column filters

Column	**Filters**
Device Name	Filter by device name. (Alphabetic)
Config Status	Filter by configuration status: • Synchronized • Synchronized from Auto Update • Out of Sync • Pending • Warning
Policy Package Status	Filter by policy package status: • Installed • Never Installed • Modified

Table 10: Column filters (continued)

Column	Filters
Connectivity	Filter by connectivity status: • Connected • Connection Down • Unknown
IP	Filter by IP. (Numeric)
Platform	Filter by platform type, e.g. FortiGate-VM. (Alphabetic)
FortiGuard License	Filter by license status: • Valid • Expired • Unknown
Logs	Filter by devices with logs.
Quota	Filter by device quota.
Log Connection	Filter by log connection status.
Firmware Version	Filter by firmware version.
Other	Filter by Description, Contact, City, Province, Country, Company.

Column settings applies to the horizontal view only. The vertical view has a quick filter option beside the search window where you can select *View All, Connection Down, Config Changed,* and *License Expired*.

View managed devices

You can view information about individual devices in the FortiManager *Device Manager* tab. This section describes the FortiGate unit summary.

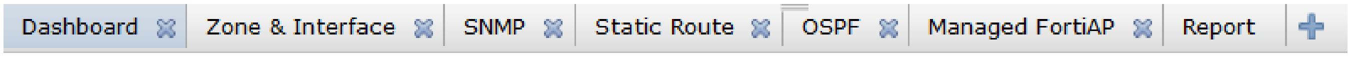
To view managed devices:

1. Select the *Device Manager* tab.
2. Select the ADOM and the device group, for example *All FortiGates,* on the tree-menu.
3. Select a FortiGate from the list of managed devices.

   The device dashboard and related information is listed on the lower portion of the content pane (or in the right-hand side content pane in vertical view).

   The dashboard toolbar displays configuration menu options for the selected device.

Figure 75: Example dashboard toolbar



Dashboard toolbar

The dashboard toolbar tabs can be customized at both the ADOM and device level.

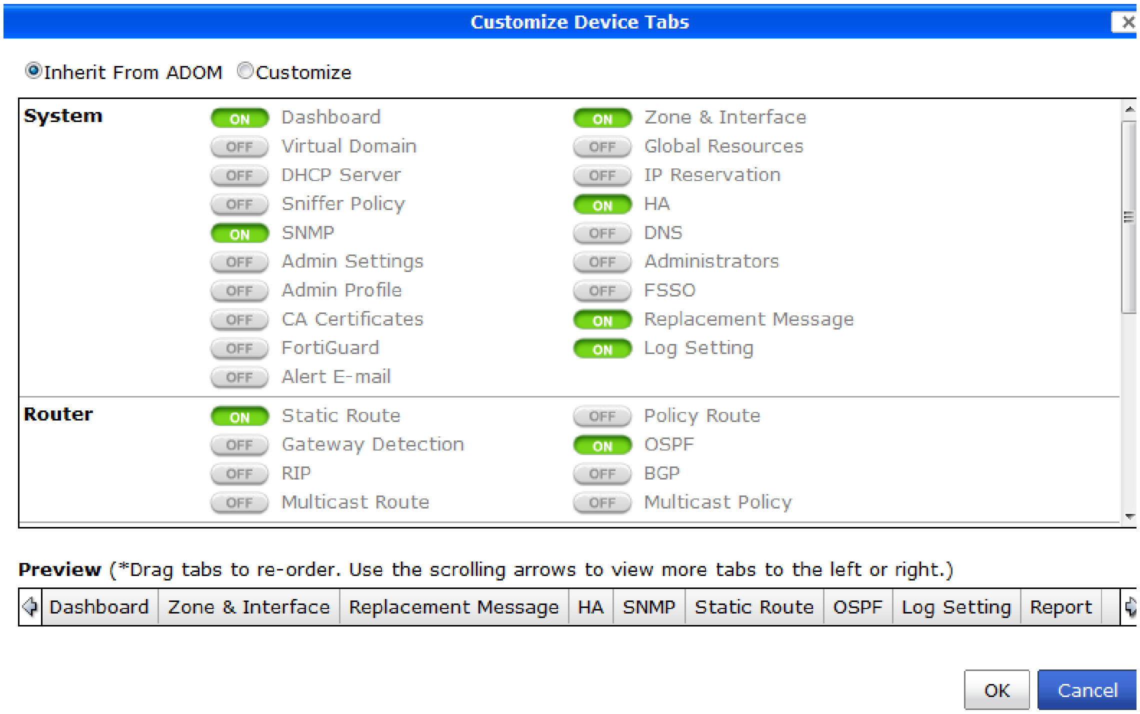
Right-click on an ADOM in the navigation tree and select *Customize Device Tabs* to customize the device tabs at the ADOM level.

Select the plus (+) symbol in the dashboard toolbar to customize the device tabs at the device level.

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

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

Figure 76: Customize tabs



Customize Device Tabs

● Inherit From ADOM ○ Customize

System	ON Dashboard	ON Zone & Interface
	OFF Virtual Domain	OFF Global Resources
	OFF DHCP Server	OFF IP Reservation
	OFF Sniffer Policy	ON HA
	ON SNMP	OFF DNS
	OFF Admin Settings	OFF Administrators
	OFF Admin Profile	OFF FSSO
	OFF CA Certificates	ON Replacement Message
	OFF FortiGuard	ON Log Setting
	OFF Alert E-mail	
Router	ON Static Route	OFF Policy Route
	OFF Gateway Detection	ON OSPF
	OFF RIP	OFF BGP
	OFF Multicast Route	OFF Multicast Policy

Preview (*Drag tabs to re-order. Use the scrolling arrows to view more tabs to the left or right.)

Dashboard | Zone & Interface | Replacement Message | HA | SNMP | Static Route | OSPF | Log Setting | Report

The following table provides an overview and descriptions of common dashboard toolbar tabs, and tab options.

System	
Dashboard	View System Information, License Information, Connection Summary, and Configuration and Installation Status device widgets.

Zone & Interface	Configure interfaces, VDOM links, zone mapping for interfaces, and intra-zone traffic.
Port Pair	Configure port pairs for transparent VDOMs.
Virtual Domain	Configure virtual domains. Set the management virtual domain.
Global Resources	Select to view virtual domain resources. Left-click on a resource entry to configure settings. Right-click a resource entry to reset the value to default.
DHCP Server	Configure DHCP server and relay service settings.
IP Reservation	Configure regular and IPsec IP/MAC address reservations.
Modem	Enable and configure USB modem settings.
Sniffer Policy	Configure sniffer policies.
HA	View high availability configuration and cluster settings.
SNMP	Create new, enable, disable, and view SNMP v1, v2c, v3 configuration.
DNS	Configure DNS or DDNS settings.
DNS Database	Create new, edit, and delete DNS zones.
Explicit Proxy	Configure explicit web proxy options. Create new web proxy forwarding servers. Configure explicit FTP proxy options.
Management	Configure the management IP address and netmask.
Admin Settings	Configure central management options.
Administrators	Create new, edit, and delete administrators.
Admin Profile	Configure administrator access profiles. Configure as global or VDOM, and set WiFi access.
FSSO	Configure FSSO agents and LDAP server settings.
Local Host ID	Configure the local host ID. Advanced options include setting the tunnel SSL algorithm and the auto detect algorithm.
CA Certificates	Configure CA certificates.
Replacement Messages	Configure replacement messages.
FortiGuard	Configure FortiGuard Distribution Network (FDN) services and settings.
FortiAnalyzer Setting	Enable or disable logging and archiving to FortiAnalyzer/FortiManager and Syslog.
Messaging Servers	Configure SMTP server settings.
Log Setting	Configure logging, and archiving settings. Enable event logging, and specify the types of events to log.

Alert E-mail	Configure alert email settings.
Router	
Routing Table	Configure static routes.
Static Route	Configure static routes.
IPv6 Static Route	Configure IPv6 static routes.
Policy Route	Configure policy routes.
Gateway Detection	Configure new dead gateway detection.
OSPF	Configure OSPF default information, redistribute. Create new areas, network, and interfaces.
RIP	Configure RIP version, add networks, create new interfaces.
BGP	Configure local AS and router ID. Add neighbors and networks.
Multicast Route	Enable multicast routing, add static rendezvous points, and create new interfaces.
Multicast Policy	Configure multicast policies.
Dynamic Objects	
Address	Configure dynamic to local address mappings.
Virtual IP	Configure dynamic virtual IP to local virtual IP mappings.
IP Pool	Configure dynamic IP pool to local IP pool mappings.
Local Certificates	Configure dynamic local certificate to VPN local certificate mappings.
VPN Tunnel	Configure dynamic VPN tunnel to VPN tunnel mappings.
WAN Opt. & Cache	
Local Host ID	Configure the local host ID.
Rule	Configure WAN optimization rules.
Peer	Configure WAN optimization peers.
Authentication Group	Configure authentication groups.
Setting	Configure cache options.
Exempt List	Configure exempt URLs.
VPN	
IPsec Phase 1	Configure IPsec phase 1 settings.
IPsec Phase 2	Configure IPsec phase 2 settings.
Manual Key	Configure manual key settings.

Concentrator	Configure concentrator settings.
SSLVPN Config	Configure SSL-VPN.
Wireless	
Managed FortiAP	Discover and authorize FortiAP devices. View managed FortiAP settings.
WiFi SSID	Configure WiFi SSID.
WIDS Profile	Configure wireless intrusion detection system profiles.
Rogue AP Settings	Enable or disable rogue AP detection and on-wire rogue AP detection technique.
Local WiFi Radio	Configure the local radio.
Custom AP Profile	Configure AP profiles.
Query	
DHCP	DHCP query including interface, IP, MAC address, VCI, expiry and status information.
IPsec VPN	IPsec VPN query including name, type, user name, incoming data, outgoing data, gateway, port, source proxy and destination proxy information. You can change the status of a connection from this tab.
SSL-VPN	SSL-VPN query information including user name, remote host, lost login time, subsession type and subsession description information.
User	User query including user name, user group, policy ID, duration, expiry, traffic volume and method information. You have the option to de authorize a user.
FortiToken	FortiToken query including the serial number and status information. You can activate a FortiToken from this tab.
Web Filter	Web filter query including protocol, requests, quarantined, email filter, banned word, file filter, antivirus, archive, FortiGuard and URL information.
Application	Application query including ID, bytes, application name and session information.
Email	Email query including protocol, requests, email filter, banned word, file filter, antivirus, archive, FortiGuard, URL filter and fragmented information.
Archive & Data Leak	Archive and data leak queries.
WiFi Clients	WiFi client query including IP, SSID, FortiAP, MAC address, authentication, vendor info, rate, signal strength, idle time and associate time information.

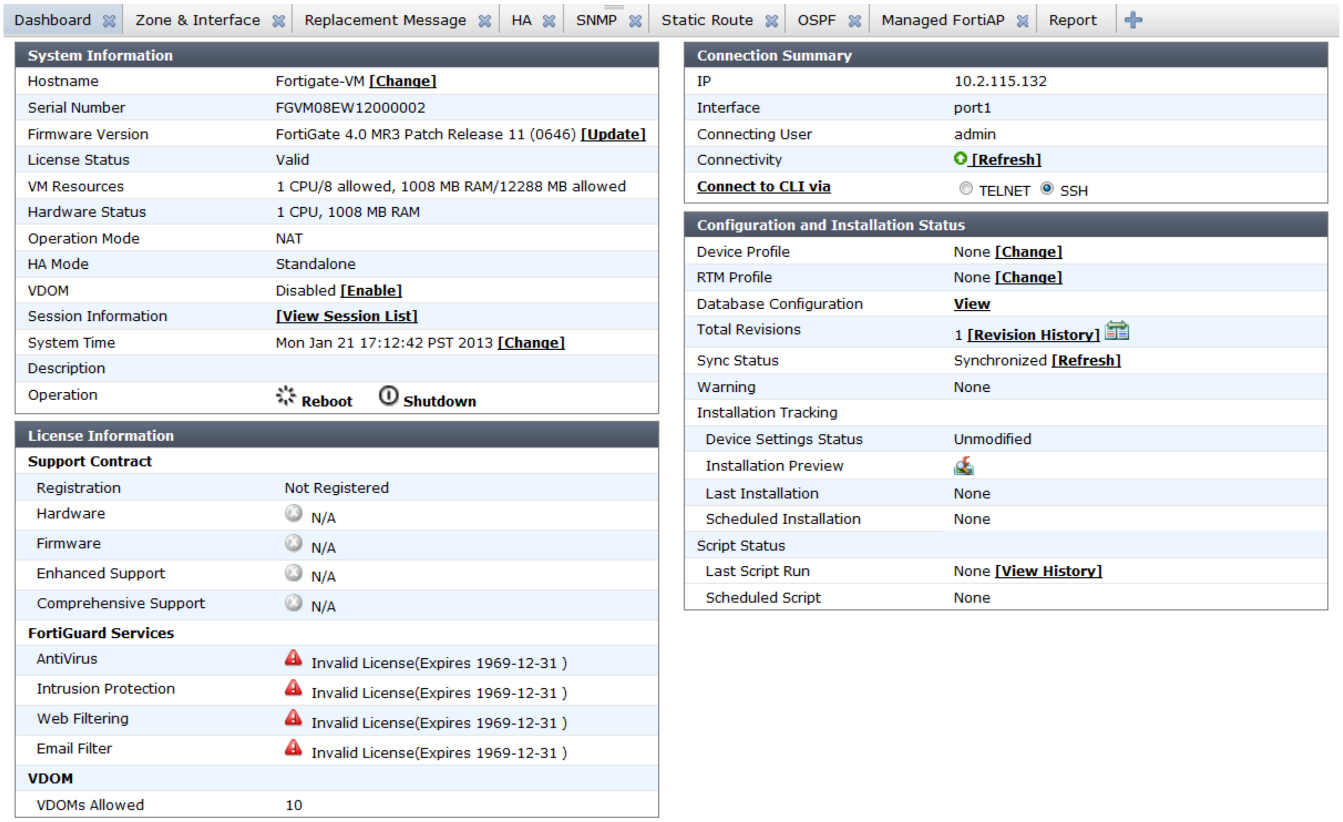
Rogue AP	Rogue AP query including state, online status, SSID, MAC address, vendor info, security type, signal strength, channel and rate information. You have the option to change the status of a connection from this tab.
Logging	Logging queries.
Report	
Report	Configure device reports.
Real-time Monitor	Select the RTM profile dashboards to include. This option is only available when an RTM profile has been assigned to the selected device.

Dashboard widgets

The dashboard widgets provide quick access to device information, and device connectivity with the FortiManager system. The following widgets are available in FortiManager v5.0:

- System Information
- License Information
- Connection Summary
- Configuration and Installation Status

Figure 77: FortiGate unit dashboard



Dashboard | Zone & Interface | Replacement Message | HA | SNMP | Static Route | OSPF | Managed FortiAP | Report

System Information	
Hostname	Fortigate-VM [Change]
Serial Number	FGVM08EW12000002
Firmware Version	FortiGate 4.0 MR3 Patch Release 11 (0646) [Update]
License Status	Valid
VM Resources	1 CPU/8 allowed, 1008 MB RAM/12288 MB allowed
Hardware Status	1 CPU, 1008 MB RAM
Operation Mode	NAT
HA Mode	Standalone
VDOM	Disabled [Enable]
Session Information	[View Session List]
System Time	Mon Jan 21 17:12:42 PST 2013 [Change]
Description	
Operation	Reboot Shutdown

License Information	
Support Contract	
Registration	Not Registered
Hardware	N/A
Firmware	N/A
Enhanced Support	N/A
Comprehensive Support	N/A
FortiGuard Services	
AntiVirus	⚠ Invalid License(Expires 1969-12-31)
Intrusion Protection	⚠ Invalid License(Expires 1969-12-31)
Web Filtering	⚠ Invalid License(Expires 1969-12-31)
Email Filter	⚠ Invalid License(Expires 1969-12-31)
VDOM	
VDOMs Allowed	10

Connection Summary	
IP	10.2.115.132
Interface	port1
Connecting User	admin
Connectivity	● [Refresh]
Connect to CLI via	○ TELNET ● SSH

Configuration and Installation Status	
Device Profile	None [Change]
RTM Profile	None [Change]
Database Configuration	View
Total Revisions	1 [Revision History]
Sync Status	Synchronized [Refresh]
Warning	None
Installation Tracking	
Device Settings Status	Unmodified
Installation Preview	
Last Installation	None
Scheduled Installation	None
Script Status	
Last Script Run	None [View History]
Scheduled Script	None

The following table provide a description of these dashboard widgets.

System Information	
Hostname	The name of the device.
Serial Number	The device serial number.
Firmware Version	The device firmware version and build number. Select [Update] to view and update the device firmware.
License Status	The license status. (VM only)
VM Resources	The number of CPU's installed, and allowed. The amount of RAM installed, and allowed. (VM only)
Operation Mode	Operational mode of the FortiGate unit: NAT or Transparent.
HA Mode	Standalone indicates non-HA mode. Active-Passive, Active-Active indicates the device is operating in a cluster. Select *Details* to view cluster settings.
Cluster Name	The name of the cluster.
Cluster Members	The hostname, serial number, role, and status of cluster members.
VDOM	The status of VDOMs on the device. Select *Enable/Disable* to toggle the VDOM role.
Session Information	Select *View Session List* to view the device session information.
System Time	The device system time and date information. Select *Change* to set time or synchronize with NTP server.
Description	Descriptive information about the device.
Operation	Select to *Reboot* or *Shutdown* the managed device.
License Information	
Support Contract	The support contract information and the expiry date. The support contract includes the following: Registration, Hardware, Firmware, and Support Level e.g. Enhanced Support, Comprehensive Support.
FortiGuard Services	The contract version, issue date and service status. FortiGuard Services includes the following: Antivirus,Intrusion protection,Web filtering, and Email filtering.
VDOM	The number of virtual domains that the device supports.
Connection Summary	
IP	The IP address of the device.
Interface	The port used to connect to the FortiManager system.
Connecting User	The user name for logging in to the device.

Connectivity	The device connectivity status and the time it was last checked. A green arrow means that the connection between the device and the FortiManager system is up; a red arrow means that the connection is down. Select *Refresh* to test the connection between the device and the FortiManager system.
Connect to CLI via	Select the method by which the you connect to the device CLI, either SSH or TELNET.
Configuration and Installation Status	
Device Profile	The device profile associated with the device. Select *Change* to set this value.
RTM Profile	The RTM profile associated with the device. Select *Change* to set this value.
Database Configuration	Select *View* to display the configuration file of the FortiGate unit.
Total Revisions	Displays the total number of configuration revisions and the revision history. Select *Revision History* to view device history.
Sync Status	The synchronization status with the FortiManager. • *Synchronized*: The latest revision is confirmed as running on the device. • *Out_of_sync*: The configuration file on the device is not synchronized with the FortiManager system. • *Unknown*: The FortiManager system is unable to detect which revision (in revision history) is currently running on the device. • Select *Refresh* to update the Installation Status.
Warning	Displays any warnings related to configuration and installation status. • *None*: No warning. • *Unknown configuration version running on FortiGate: FortiGate configuration has been changed!*: The FortiManager system cannot detect which revision (in *Revision History*) is currently running on the device. • *Unable to detect the FortiGate version*: Connectivity error! • *Aborted*: The FortiManager system cannot access the device.
Installation Tracking	
Device Settings Status	• *Modified*: Some configuration on the device has changed since the latest revision in the FortiManager database. Select *Save Now* to install and save the configuration. • *UnModified*: All configuration displayed on the device is saved as the latest revision in the FortiManager database.
Installation Preview	Select icon to display a set of commands that will be used in an actual device configuration installation in a new window.

Last Installation	*Last Installation*: The FortiManager system sent a configuration to the device at the time and date listed.
Scheduled Installation	*Scheduled Installation*: A new configuration will be installed on the device at the date and time indicated.
Script Status	Select Configure to view script execution history.
Last Script Run	Displays the date when the last script was run against the managed device.
Scheduled Script	Displays the date when the next script is scheduled to run against the managed device.

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

Administrative domains (ADOMs)

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

- Firmware version: group all v5.0 devices into one ADOM, and all v4.0 MR3 into another.
- Geographic regions: group all devices for a specific geographic region into an ADOM, and devices for a separate region into another ADOM.
- Admin users: group devices into separate ADOMs based for specific administrators responsible for the group of devices.
- Customers: group all devices for one customer into an ADOM, and devices for another customer into another ADOM.
- Device type: create a separate ADOM for each device type, i.e. FortiGate, FortiCarrier, and FortiSwitch.

Each admin profile can be customized to provide read-only, read-write, or restrict access to various ADOM settings. When creating new admin accounts, you can restrict which ADOMs the administrator can access, for enhanced control of your admin users. For more information on ADOM configuration and settings, see “Administrative Domains” on page 41.

For information on adding devices to an ADOM using the *Add Device* wizard, see “FortiManager Wizards” on page 158.

Managing devices

To manage a device, you must add it to the FortiManager system. You also need to enable *Central Management* on the managed device. You can add an existing operational device, an unregistered device, or provision a new device.

Once a device has been added to the ADOM on the *Device Manager* tab, the configuration is available within other tabs in the FortiManager system including *Policy & Objects*, *Log View*, and *Reports*.

This section includes the following topics:

- Adding a device
- Replacing a managed device
- Editing device information
- Refreshing a device
- Install policy package and device settings
- Importing and exporting device lists
- Setting unregistered device options

Adding a device

You can add individual devices, or multiple devices. When adding devices using the *Add Device* wizard you have more configuration options then using the *Add Multiple* option.

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

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

To add a device to an ADOM:

1. Right-click on the tree-menu, and select *Add Device*.
2. Select Discover for a device which is online. Select Add Model Device to provision a device which is not yet online.
3. Follow the steps in the wizard to add the device to the ADOM.

For detailed information on adding devices to an ADOM using the *Add Device* wizard, see "FortiManager Wizards" on page 158.

Replacing a managed device

The serial number will be verified before each management connection. In the event of a replaced device, it is necessary to manually change the serial number in the FortiManager system and re-deploy the configuration.

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

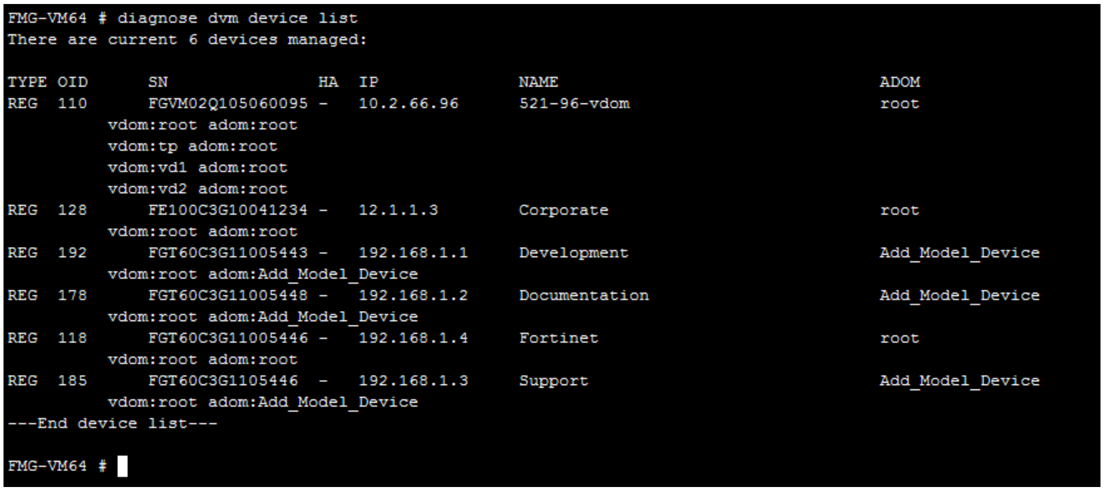
View all managed devices from the CLI

To view all devices that are being managed by your FortiManager, use the following command:

```
diagnose dvm device list
```

The output lists the number of managed devices, device type, OID, device serial number, VDOMs, HA status, IP address, device name, and the ADOM to which the device belongs.

Figure 78: View all managed devices from the CLI



```
FMG-VM64 # diagnose dvm device list
There are current 6 devices managed:

TYPE OID      SN              HA  IP            NAME                               ADOM
REG  110      FGVM02Q105060095 -   10.2.66.96    521-96-vdom                        root
         vdom:root adom:root
         vdom:tp adom:root
         vdom:vd1 adom:root
         vdom:vd2 adom:root
REG  128      FE100C3G10041234 -   12.1.1.3      Corporate                          root
         vdom:root adom:root
REG  192      FGT60C3G11005443 -   192.168.1.1   Development                        Add_Model_Device
         vdom:root adom:Add_Model_Device
REG  178      FGT60C3G11005448 -   192.168.1.2   Documentation                      Add_Model_Device
         vdom:root adom:Add_Model_Device
REG  118      FGT60C3G11005446 -   192.168.1.4   Fortinet                           root
         vdom:root adom:root
REG  185      FGT60C3G1105446  -   192.168.1.3   Support                            Add_Model_Device
         vdom:root adom:Add_Model_Device
---End device list---

FMG-VM64 #
```

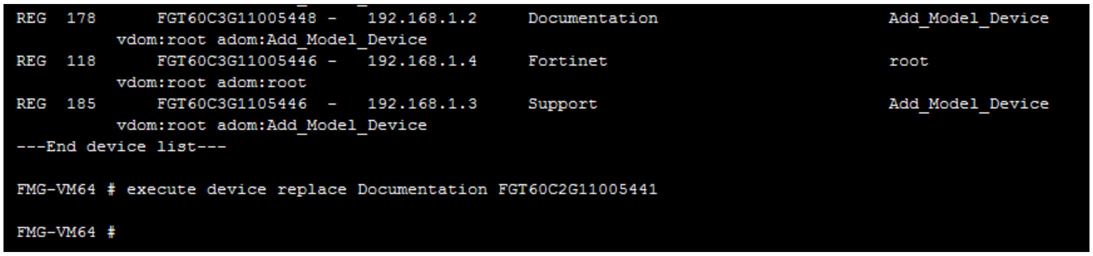
Changing the serial number from the CLI

If the device serial number was entered incorrectly using the *Add Model Device* wizard, you can replace the serial number from the CLI only. Use the command:

```
execute device replace sn <device name> <serial number>
```

This command is also useful when performing an RMA replacement.

Figure 79: Change the serial number of a managed device



```
REG  178      FGT60C3G11005448 -   192.168.1.2   Documentation                      Add_Model_Device
         vdom:root adom:Add_Model_Device
REG  118      FGT60C3G11005446 -   192.168.1.4   Fortinet                           root
         vdom:root adom:root
REG  185      FGT60C3G1105446  -   192.168.1.3   Support                            Add_Model_Device
         vdom:root adom:Add_Model_Device
---End device list---

FMG-VM64 # execute device replace Documentation FGT60C2G11005441

FMG-VM64 #
```

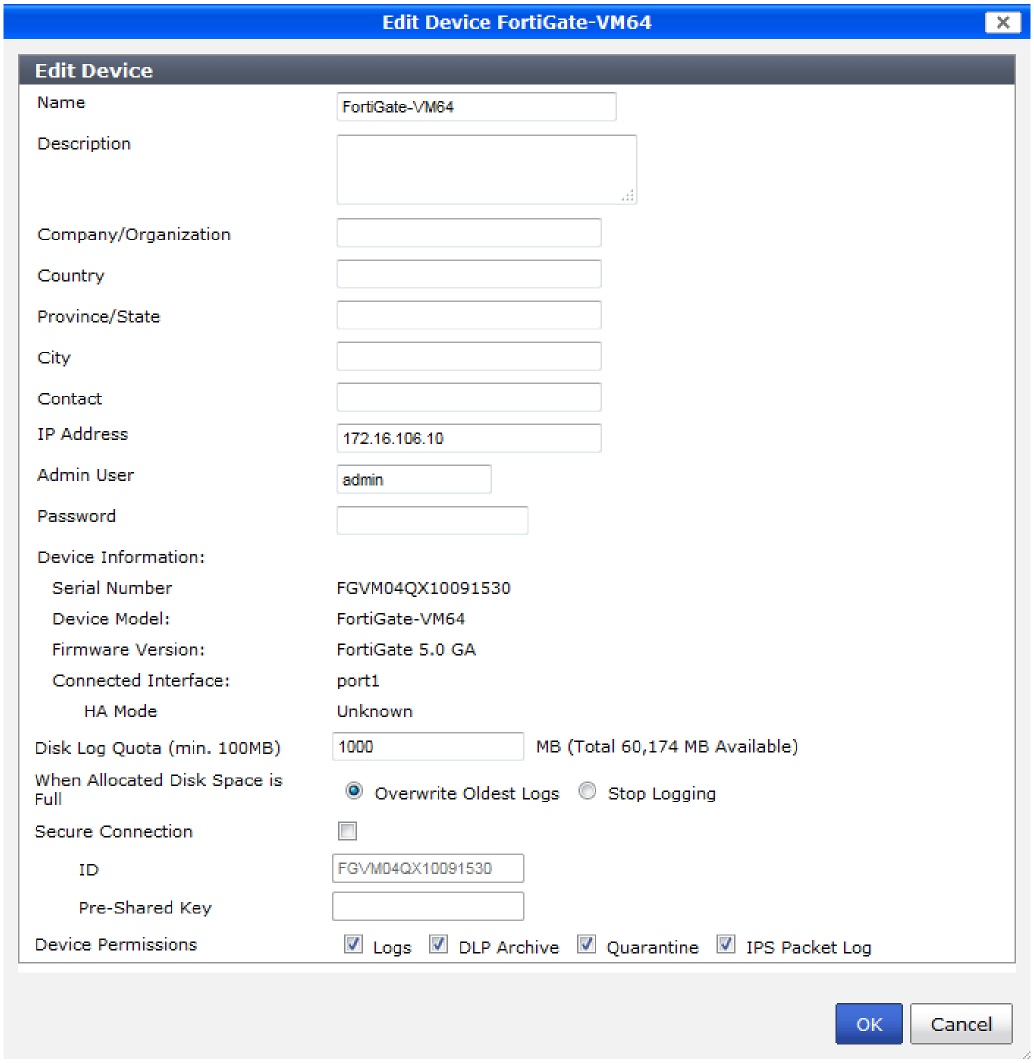
Editing device information

You can edit device information including the *Name*, *Description*, *IP address*, *Admin User*, and *Password*.

To edit information for a single device:

1. On the tree menu, select the ADOM, and device group.
2. Select a device from the device list then select the *Edit* icon, or right-click on the device row and select *Edit* from the right-click context menu.

Figure 80: Edit a device



Edit Device FortiGate-VM64

Edit Device

Name	FortiGate-VM64
Description	
Company/Organization	
Country	
Province/State	
City	
Contact	
IP Address	172.16.106.10
Admin User	admin
Password	
Device Information:	
Serial Number	FGVM04QX10091530
Device Model:	FortiGate-VM64
Firmware Version:	FortiGate 5.0 GA
Connected Interface:	port1
HA Mode	Unknown
Disk Log Quota (min. 100MB)	1000 MB (Total 60,174 MB Available)
When Allocated Disk Space is Full	● Overwrite Oldest Logs ○ Stop Logging
Secure Connection	□
ID	FGVM04QX10091530
Pre-Shared Key	
Device Permissions	☑ Logs ☑ DLP Archive ☑ Quarantine ☑ IPS Packet Log

3. Edit the following settings as required.

Name	The name of the device.
Description	Descriptive information about the device.
Company /Organization	Company or organization information.
Country	Enter the country.
Province/State	Enter the province or state.

City	Enter the city.
Contact	Enter the contact name.
IP Address	The IP address of the device.
Admin User	The admin user username.
Password	The admin user password
Device Information	Information about the device, including serial number, device model, firmware version, connected interface, HA mode, cluster name, and cluster members.
Disk Log Quota	The amount of space that the disk log is allowed to use, in MB.
When Allocated Disk Space is Full	The action for the system to take when the disk log quota is filled.
Secure Connection	Select check box to enable this feature. Secure Connection secures OFTP traffic through an IPsec tunnel.
ID	The ID is the device serial number.
Pre-Shared Key	The pre-shared key for the IPsec connection between the FortiGate and FortiManager.
Device Permissions	The device’s permissions.

4. After making the appropriate changes select *Apply*.

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

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

See also

- Importing and exporting device lists

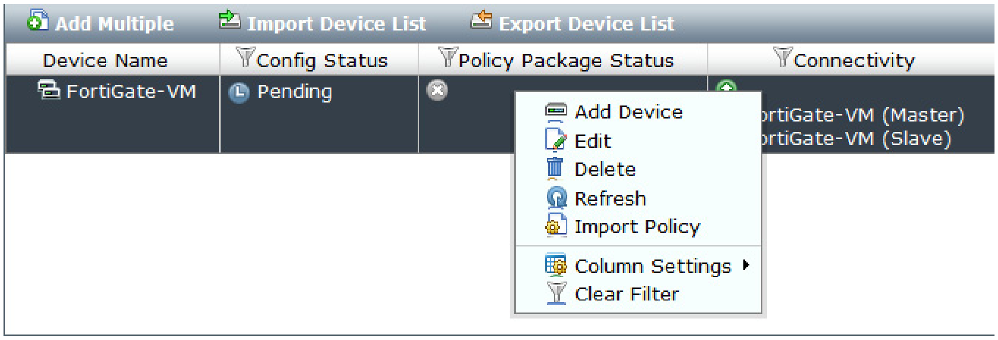
Refreshing a device

Refreshing a device refreshes the connection between the selected devices and the FortiManager system. This operation updates the device status and the FortiGate HA cluster member information.

To refresh a device:

1. In the content pane, right-click on the device.

Figure 81: Device manager right-click context menu

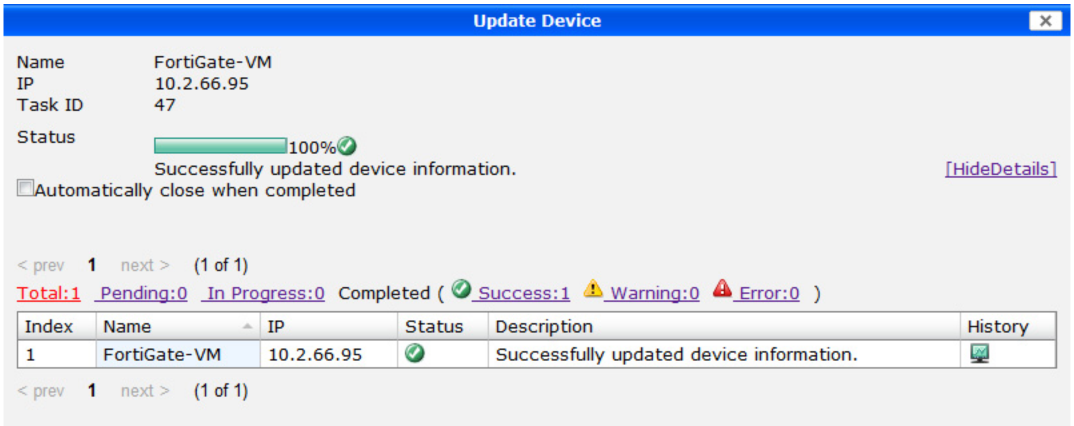


Device Name	Config Status	Policy Package Status	Connectivity
FortiGate-VM	Pending	✕	● rtiGate-VM (Master) rtiGate-VM (Slave)

2. Select *Refresh* from the context menu.

   The *Update Device* dialog box will open with update details.

Figure 82: Update device dialog box



Name	FortiGate-VM
IP	10.2.66.95
Task ID	47
Status	100% ✓ Successfully updated device information.

[HideDetails]

☐ Automatically close when completed

< prev 1 next > (1 of 1)

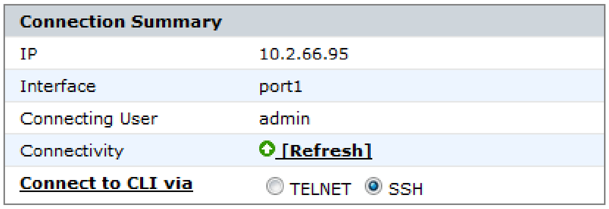
Total:1 Pending:0 In Progress:0 Completed (✓ Success:1 ⚠ Warning:0 ⚠ Error:0)

Index	Name	IP	Status	Description	History
1	FortiGate-VM	10.2.66.95	✓	Successfully updated device information.	

< prev 1 next > (1 of 1)

3. You can also select *Refresh* on the Connection Summary widget.

Figure 83: Connection Summary widget



Connection Summary	
IP	10.2.66.95
Interface	port1
Connecting User	admin
Connectivity	● [Refresh]
Connect to CLI via	○ TELNET ● SSH

Install policy package and device settings

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

To import policies to a device:

1. Right-click on the tree-menu device entry, and select *Install* on the context menu.
2. Select *Install Policy Packages & Device Settings*.

   This option will install a selected policy package to the device. Any device specific settings for devices associated with the policy package will also be installed.
3. Follow the steps in the wizard to install the policy package to the device.

For information on importing policy packages and device settings to a device using the *Install* wizard, see "FortiManager Wizards" on page 158.

Importing and exporting device lists

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

The *Import and Export Device List* features are disabled by default. To enable, go to *System Settings > Admin > Admin Settings*, and enable *Show Device List Import/Export* under *Miscellaneous Options*.

Advanced configuration settings such as zone mappings, dynamic interface bindings are not part of import/export device lists. Use the backup/restore function to backup the FortiManager configuration.

There are two ways to create the text file:

- *Export Device List*: Use this feature to save a list of devices in a text file as a backup that can be imported later.
- Create the file manually: For more information, see "Example text files" on page 140.

To import a device list:

1. Select the *Device Manager* tab.
2. On the content pane toolbar, select *Import Device List*.
3. Select *Browse* and locate and specify the device list text file.
4. Select *Submit*.

To export a device list:

1. Select *Device Manager* tab.
2. On the content pane toolbar, select *Export Device List*.
3. Save the file.

Import text file general 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 device:

```
device_list_ver=8
```

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 importing 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.

ADOM file format

ADOMs are specified by the following ADOM lines:

```
device_list_ver=8
adom|name|mode|status|version|mr|migration_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 139.

Field Name	Blank Allowed	Description
name	No	Name of the ADOM.
mode	No	In FortiManager v5.0 the mode is GMS. This field reflects legacy code.
status	No	Enter 1 to enable the ADOM. Enter 0 to disable the ADOM..
version	No	The ADOM version, for example, 5.0.
mr	No	Major Release designation of the device. For example, GA, MR1, MR2.
migration mode	No	In FortiManager v5.0 the value is 0. This field reflects legacy code.
enable	No	Enter 1 to enable, 0 to disable.

mode is a legacy field, *GMS* must be entered as the value.
migration mode is also a legacy field, *5.0* must be entered as the value.

Device file format

Devices are specified by the following device lines:

```
device_list_ver=8
device|ip|name|platform|admin|passwd|adom|desc|discover|reload|fwver
    |mr|patch|build|branch_pt|interim|sn|has_hd|faz.quota|faz.perm|
```

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.
name	No	Device name.
platform	No	The device type. For example, FortiGate, or the full platform name: FortiWiFi-60B.
admin	No	Administrator username.
passwd	Yes	Administrator 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.
mr	No	Major Release designation of the device. For example, GA, MR1, MR2.
patch	No	Patch level.
build	No	The four digit build number
branch_pt	No	The firmware branch point. You can find this information from the FortiOS CLI command get system status.
sn	No	Device serial number.
has_hd	No	Enter 1 if the device has a hard disk, 0 if the device does not.

faz.quota	No	The disk log quota in MB.
faz.perm	No	The device permissions. DVM_PERM_LOGS : Permission to receive and store log messages DVM_PERM_DLP_ARCHIVE : Permission to receive and store dlp archive files DVM_PERM_QUARANTINE : Permission to receive and store quarantine files DVM_PERM_IPS_PKT_LOG : Permission to receive and store IPS packet log

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 139), 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 v4.0.

Group file format

Device group are specified as follows:

```
device_list_ver=8
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 139.

```
+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 two levels of group nestings are permitted in FortiManager v4.0.

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.

Example 1: Device

```
device_list_ver=8
# 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-400C|admin|password|adom01|Your
     description.|0|1|5.0|GA|FG400C2905550018|0|
+meta|bogosity|12|
+vdom|vdom01|adom01|
```

Example 2: ADOM

```
device_list_ver=8
# 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|GMS|1|
+meta|tag|your domain|
```

Example 3: Device group

```
device_list_ver=8
# 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|Philip J. Fry|
+member|top|vdom01|
+member|top|vdom02|
+subgroup|group01|

group|group03||adom01|
+meta|supervisor|Bender B. Rodriguez|
```

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

Setting unregistered device options

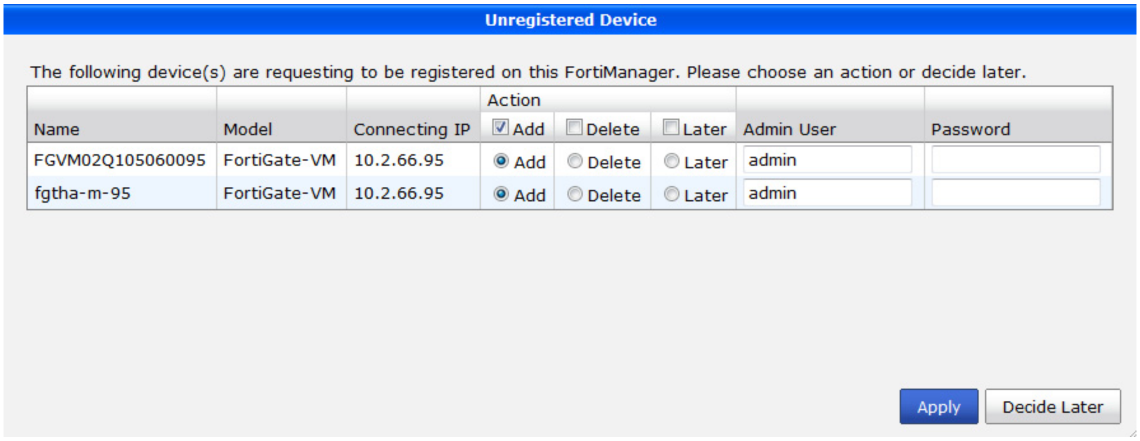
In FortiManager v5.0, setting unregistered device options is from the CLI only. Enter the following command to enable or disable allowing unregistered devices to be registered with the FortiManager.

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

allow register [enable | disable]	Enable or disable registration of an unregistered device.
unreg_dev_opt	Set the action to take when an unregistered device connects to the FortiManager
add_allow_service	Add unregistered devices and allow service requests.
add_no_service	Add unregistered devices but deny service requests.

When the `set allow register` command is set to `disable`, you will not receive the following unregistered device dialog box.

Figure 84: Unregistered device dialog box on login



Unregistered Device

The following device(s) are requesting to be registered on this FortiManager. Please choose an action or decide later.

			Action				
Name	Model	Connecting IP	☑ Add	☐ Delete	☐ Later	Admin User	Password
FGVM02Q105060095	FortiGate-VM	10.2.66.95	● Add	○ Delete	○ Later	admin	
fgtha-m-95	FortiGate-VM	10.2.66.95	● Add	○ Delete	○ Later	admin	

Configuring devices

You can configure the FortiGate units in three ways:

- Per device, from the *Device Manager* dashboard toolbar.
- Per VDOM, from the *Device Manager* dashboard toolbar.
- Per device profile.

This section contains the following topics:

- Configuring a device
- Configuring virtual domains (VDOMs)
- Device profiles

Configuring a device

Configuring a FortiGate unit using the *Device Manager* dashboard toolbar 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.

This document does not provide detailed procedures for configuring FortiGate units. See the FortiGate documentation for complete information. The most up-to-date FortiGate documentation is also available from the Fortinet Technical Documentation web page.

To configure a FortiGate unit:

1. On the *Device Manager* tab, select the ADOM and the unit you want to configure on the tree-menu.
2. Select an option for that unit in the dashboard toolbar.
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.

You can rename and reapply firewall objects after they are created and applied to a firewall policy. When you do so, the FortiManager system will:

- delete all dependencies
- delete the object
- recreate a new object with the same value, and
- recreate the policy to reapply the new object.

Firewall policy reordering on first installation

On the first discovery of a FortiGate unit, the FortiManager system will retrieve the unit's configuration and load it into the *Device Manager*. After you make configuration changes and install them, you may see that the FortiManager system reorders some of the firewall policies in the FortiGate unit’s configuration file.

This behavior is normal for the following reasons:

- The FortiManager system maintains the order of policies in the actual order you see them and manipulate them in the 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*..

In FortiManager v5.0, VDOMs have their own dashboard and toolbar. You can configure the VDOM in the same way as configuring a device.

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

Creating and editing virtual domains

Creating and editing virtual domains in the 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. On the *Device Manager* tab, select the unit you want to configure.
2. On the device dashboard toolbar, go to *Dashboard* > *System Information*.
3. Select the *Enable* link in the *Virtual Domain* field.

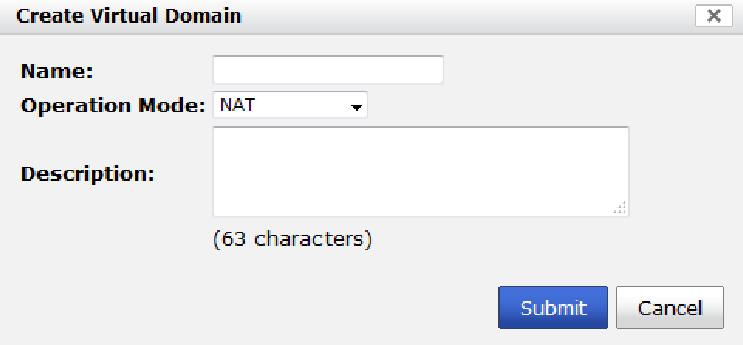
To create a virtual domain:

1. In the *Device Manager* tab, select the unit you want to configure.
2. In the lower content pane tab bar, go to the *Virtual Domain* tab, then select *Create New* to create a new VDOM.

The Virtual Domain tab may not be visible in the lower content pane tab bar. See "View managed devices" on page 121 for more information.

After the first VDOM is created you can create additional VDOMs by right-clicking on the exisiting VDOM and selecting *Add VDOM* from the right-click menu.

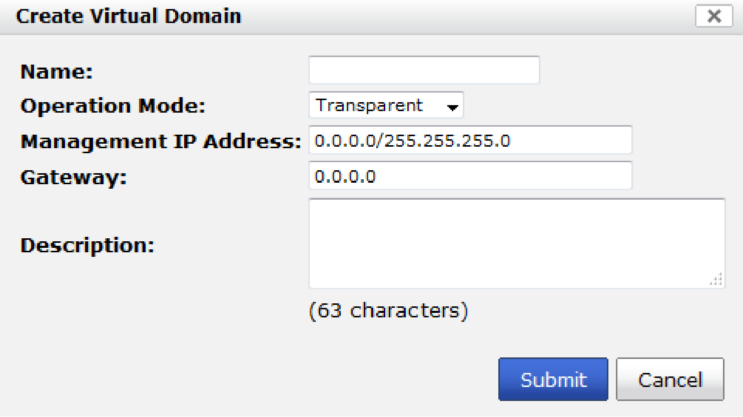
Figure 85: Create a new NAT VDOM



Create Virtual Domain

Name:	
Operation Mode:	NAT
Description:	
	(63 characters)

Figure 86: Create a new transparent VDOM



Create Virtual Domain

Name:	
Operation Mode:	Transparent
Management IP Address:	0.0.0.0/255.255.255.0
Gateway:	0.0.0.0
Description:	
	(63 characters)

3. Enter the name, operation mode and an optional description for the new VDOM. If you selected Transparent mode, you also need to enter the management IP and mask, as well as the gateway.
4. Select *Submit* to create the new VDOM.

Configuring inter-VDOM routing

By default, for two virtual domains to communicate it must be through externally connected physical interfaces. Inter-VDOM routing creates a link with two ends that act as virtual interfaces, internally connecting the two virtual domains.

Before configuring inter-VDOM routing:

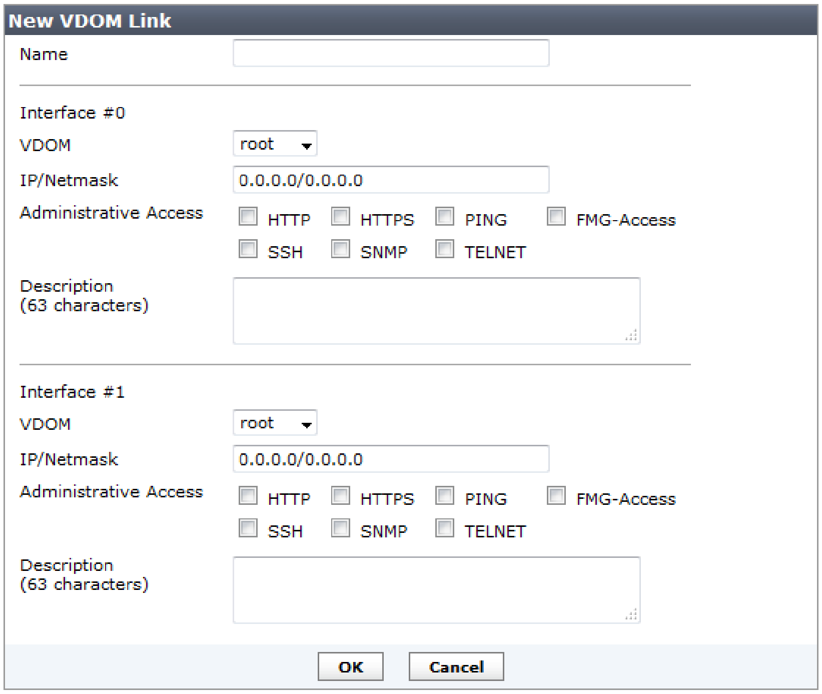
- You must have at least two virtual domains configured.
- The virtual domains must all be in NAT mode.
- Each virtual domain to be linked must have at least one interface or subinterface assigned to it.

To create a VDOM link:

1. In the *Device Tree*, select a virtual domain.
2. Select the *Zone & Interface* tab.
3. Select *Create New* > *VDOM Link* from the toolbar.

   The *New VDOM Link* window opens.

Figure 87: New VDOM link



New VDOM Link

Name

Interface #0

VDOM: root

IP/Netmask: 0.0.0.0/0.0.0.0

Administrative Access: □ HTTP □ HTTPS □ PING □ FMG-Access □ SSH □ SNMP □ TELNET

Description (63 characters)

Interface #1

VDOM: root

IP/Netmask: 0.0.0.0/0.0.0.0

Administrative Access: □ HTTP □ HTTPS □ PING □ FMG-Access □ SSH □ SNMP □ TELNET

Description (63 characters)

4. Enter the following information:

Name	Name of the VDOM link.
Interface #x	The interface number, either *1* or *0*.
VDOM	Select the VDOM

IP/Netmask	Enter the IP address and netmask for the VDOM.
Administrative Access	Select the allowed administrative service protocols from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, and Web Service.
Description	Optionally, enter a description for the link.

5. Select *OK* to save your settings.

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.

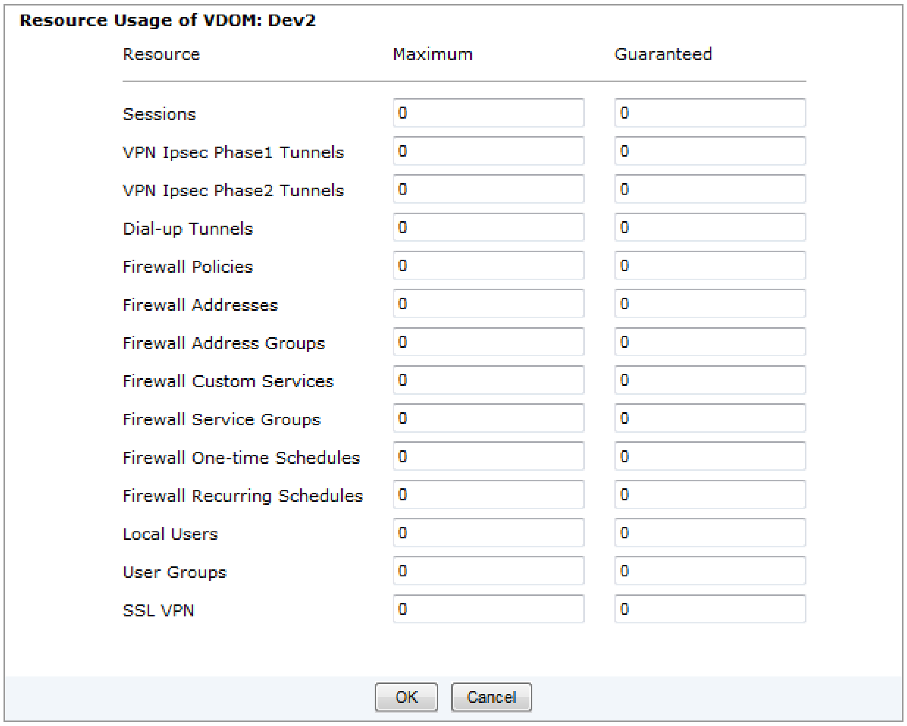
For more information, see "Configuring VDOM global resources" on page 147.

To configure a VDOM's resource limits:

1. On the *Device Manager* tab, select the unit you want to configure.
2. Select the *Virtual Domain* tab in the lower content pane, then select the *Resource* icon for one of the VDOMs in the list.

   The *Resource Usage* page opens.

   Figure 88: Resource usage page



Resource Usage of VDOM: Dev2

Resource	Maximum	Guaranteed
Sessions	0	0
VPN Ipsec Phase1 Tunnels	0	0
VPN Ipsec Phase2 Tunnels	0	0
Dial-up Tunnels	0	0
Firewall Policies	0	0
Firewall Addresses	0	0
Firewall Address Groups	0	0
Firewall Custom Services	0	0
Firewall Service Groups	0	0
Firewall One-time Schedules	0	0
Firewall Recurring Schedules	0	0
Local Users	0	0
User Groups	0	0
SSL VPN	0	0

3. 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.
4. Select *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* tab, select the unit you want to configure.
2. In the lower content pane, select the *Global Resources* tab.

Resource	The network resources that the VDOMs can use. Select the resource name to edit the configured value.
Configured Maximum	The maximum resource limit for all VDOMs set by the user. Unlimited is represented by a *0*.
Default Maximum	The default maximum resource limit for all VDOMs. Unlimited is represented by a *0*.
Reset	Right-click and select *Reset* to set the configured values to their default values.

Device profiles

A device profile is a subset of a model device configuration. Each device or device group will be able to be linked with a device profile. When linked, the selected settings will come from the profile, not from the *Device Manager* database.

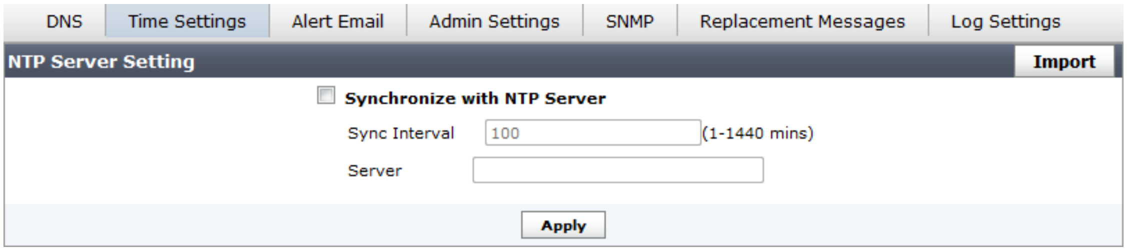
By default, there is one generic profile defined. Device profiles are managed in a similar manner to policy packages. You can use the context menus to create new device profiles.

Device profiles will support the following settings:

- DNS
- Time settings (NTP settings)
- Alert email
- Admin settings
- SNMP
- Replacement messages (Global only, you can customize per VDOM replacement messages)
- Log settings

Go to the *Device Manager* tab, then select the *Provision Profiles* section in the tree menu to configure device profiles.

Figure 89: Device profiles



NTP Server Setting

□ Synchronize with NTP Server

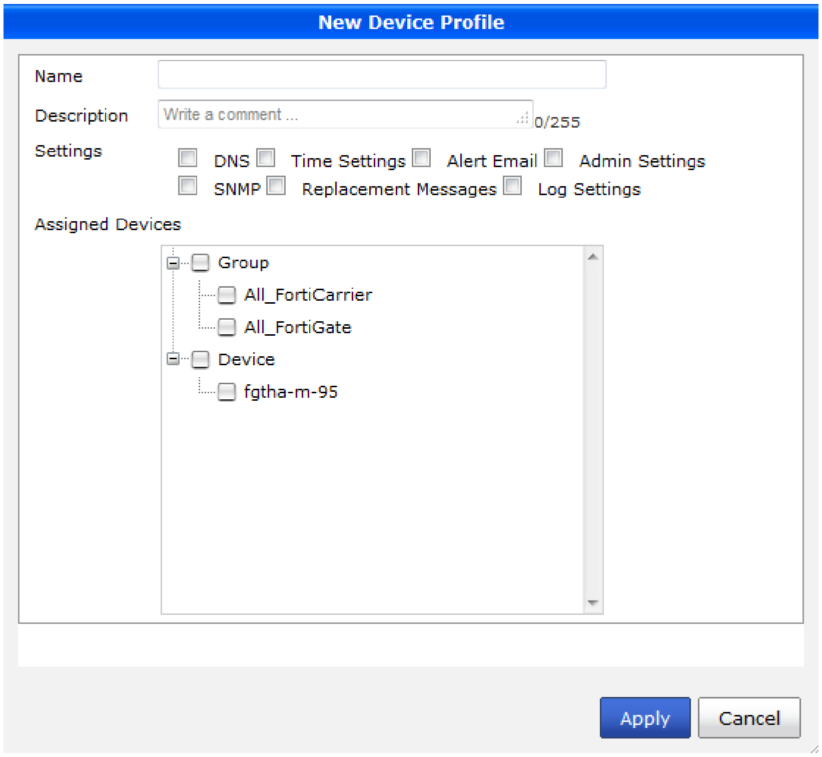
Sync Interval 100 (1-1440 mins)

Server

You can create, edit, or delete profiles by right-clicking on a profile. You can then select particular devices that will be associated with the profile.

You can link a device to the device profile using the *Add Device Wizard*, from the device's dashboard page in *Device Manager*, or by right-clicking and editing the profile and selecting devices.

Figure 90: New device profile



New Device Profile

Name

Description Write a comment ... 0/255

Settings □ DNS □ Time Settings □ Alert Email □ Admin Settings □ SNMP □ Replacement Messages □ Log Settings

Assigned Devices

- □ Group
  - □ All_FortiCarrier
  - □ All_FortiGate
- □ Device
  - □ fgtha-m-95

Log arrays

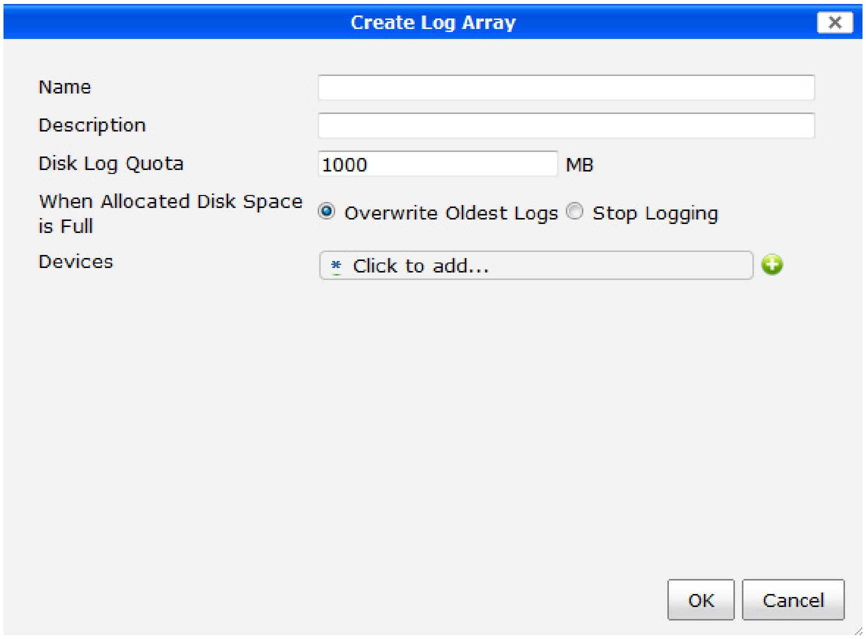
Log arrays support group-based access to logs and reports. Log arrays are available in the *Device Manager* tab. Log arrays also allow you to manage log data belonging to FortiGate HA clusters from a single device object. You can configure RTM profiles and schedule reports for each log array.

To create a new log array:

1. In the *Device Manager* tab, right-click on *All Log Arrays* and select *Add Log Array* in the right-click menu.

   The *Create Log Array* window appears.

Figure 91: Create log array window



Name

Description

Disk Log Quota 1000 MB

When Allocated Disk Space is Full ● Overwrite Oldest Logs ○ Stop Logging

Devices Click to add...

2. Configure the following settings:

Name	The name of the log array.
Description	Descriptive information about the log array.
Disk Log Quota (MB)	Enter the disk log quota in MB.
When Allocated Disk Space is Full	Select to overwrite the oldest logs or to stop logging when the allocated disk space is full.
Devices	Select the plus (+) sign to add devices or VDOMs to the log array. Each device can only belong to one log array. If the device you want to add is currently assigned to another log array, you must first remove the device from the other log array.

3. Select OK to save the log array configuration.

To edit a log array:

1. In the *Device Manager* tab, select *All Log Arrays*.
2. In the right content pane, right-click the log array you would like to edit and select *Edit* from the right-click menu.
3. Edit the settings as required.
4. Select *OK* to save the changes

To delete a log array:

1. In the *Device Manager* tab, select *All Log Arrays*.
2. In the right content pane, right-click the log array you would like to delete and select *Delete* on the right-click menu.
3. Select *OK* in the confirmation window to delete the log array.

Working with device groups

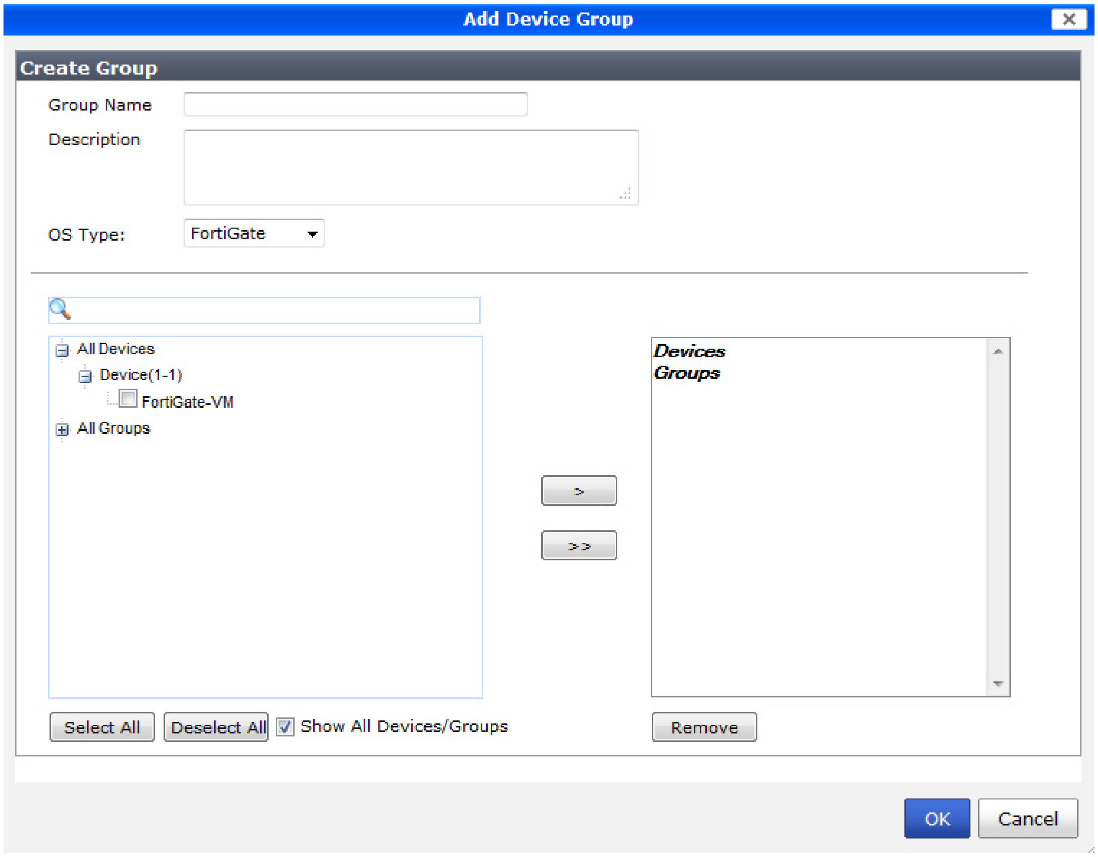
Device groups can be added, deleted, and edited as required to assist you in organized your managed devices.

To add a device group:

1. Right-click on a device group in the tree menu and select *Create New* under the *Device Group* heading in the right-click menu.

   The add *Device Group window* opens.

   Figure 92: Adding a group



OS Type: FortiGate

☑ Show All Devices/Groups

2. Complete the following fields:

Group Name	Enter a unique name for the group (maximum 32 characters). The name cannot be the same as the name of another device or device group and may only contain numbers, letters, and the special characters '-' and '_'.
Description	Enter a description for the group. The description can be used to provide more information about the group, such as its location.
OS Type	Select an OS type from the drop-down list.
Add icon	Move the selected device or group from the device list to the group member list.
Select All	Select all the devices in the device list.

Deselect All	Clear the selections in the device list.
Show All Devices/Groups	Select to display all the of the device and groups in the device list.
Remove	Clear the selected devices in the group member list.

3. Select *OK* to add the group.

To edit information for a single device group:

1. Right-click on a device group in the tree menu and select *Edit* under the *Device Group* heading in the right-click menu.

   The *Edit Device Group* window opens.
2. Make the required changes, then select *Apply*.

To delete a device group

1. Right-click on a device group in the tree menu and select *Delete* under the *Device Group* heading in the right-click menu.
2. Select *OK* in the confirmation dialog box to delete the group.

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

Managing FortiGate chassis devices

The FortiManager 5001A AdvancedTCA (ATCA) system can work with the Shelf Manager to manage FortiGate 5050, 5060, 5140, and 5140B chassis. The Shelf Manager runs on the Shelf Management Mezzanine hardware platform included with the FortiGate 5050, 5060, 5140, and 5140B chassis. You can install up to five FortiGate 5000 series blades in the five slots of the FortiGate 5050 AdvancedTCA (ATCA) chassis and up to 14 FortiGate 5000 series blades in the 14 slots of the FortiGate 5140 AdvancedTCA (ATCA) chassis. For more information on FortiGate 5000 series including Chassis and Shelf manager, see the Technical Documentation site http://docs.fortinet.com/fgt_5000.html.

FortiManager-VM-1000-UG, -5000UG and -U-UG support Shelf Manager for chassis management

You need to enable chassis management before you can work with the Shelf Manager through the FortiManager system.

To enable chassis management:

1. In the *System Settings* tab, go to *System Settings > Advanced > Advanced Settings*. See “Advanced settings” on page 103 for more information.
2. Under *Advanced Settings*, select *Chassis Management*.
3. Set the *Chassis Update Interval*; the value can be from 4 to 1440 minutes.

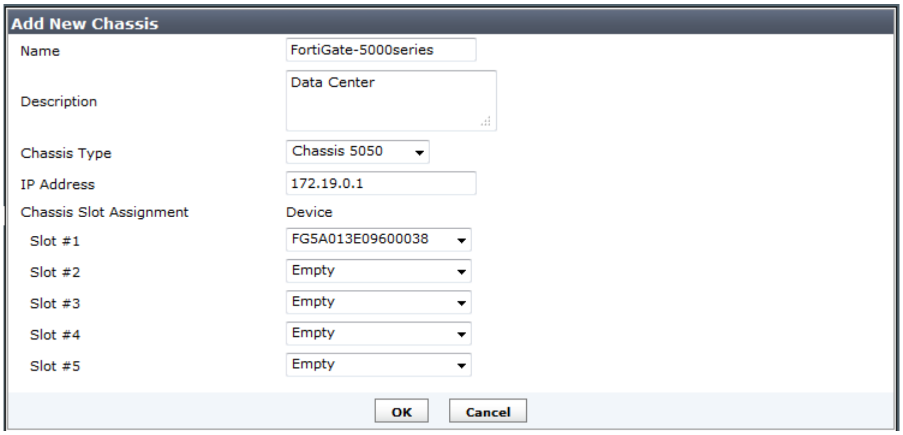
To view the chassis list, in the *Device Manager* tab, select *All Chassis* from the tree menu.

Add Chassis	Select to add a new chassis. For more information, see “To add a chassis:” on page 152.
Delete	Select the check box beside a chassis that you want to delete, then select *Delete* to remove it.
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 managed device” on page 120.
Name	Select the name of the chassis to display the blades in that chassis. See “Viewing the status of the FortiGate blades” on page 153.
Model	The model of a chassis.
IP	The IP address of the Shelf Manager running on the chassis.
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 153.
Update icon	Select to refresh the connection between a Shelf Manager and the FortiManager system.

To add a chassis:

1. in the *Device Manager* tab, select *All Chassis* from the tree menu.
2. In the content pane, select *Add Chassis* from the toolbar.

Figure 93: Add a new chassis



Add New Chassis

Name	FortiGate-5000series
Description	Data Center
Chassis Type	Chassis 5050
IP Address	172.19.0.1
Chassis Slot Assignment	Device
Slot #1	FG5A013E09600038
Slot #2	Empty
Slot #3	Empty
Slot #4	Empty
Slot #5	Empty

3. Complete the following fields:

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, 5060, 5140 or 5140B.

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 153.

4. Select *OK*.

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

1. In the navigation pane, go to *Device Manager* > *All Chassis.*
2. In the content pane, select the *Edit* icon of the chassis to edit.
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.

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 navigation pane, go to *Device Manager* > *All 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.

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

State	Indicates whether the card in the slot is installed or running, or if the slot is empty.
Temperature Sensors	Indicates if the temperature sensors for the blade in each slot are detecting a temperature within an acceptable range. *OK* indicates that all monitored temperatures are within acceptable ranges. *Critical* indicates that a monitored temperature is too high (usually about 75°C or higher) or too low (below 10°C).
Current Sensors	Indicates if the current sensors for the blade in each slot are detecting a current within an acceptable range. *OK* indicates that all monitored currents are within acceptable ranges. *Critical* indicates that a monitored current is too high or too low.
Voltage Sensors	Indicates if the voltage sensors for the blade in each slot are detecting a voltage within an acceptable range. *OK* indicates that all monitored voltages are within acceptable ranges. *Critical* indicates that a monitored voltage is too high or too low.
Power 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 154.
Browse icon	Select to update the slot.

To edit voltage and temperature values:

1. Go to *Device Manager* > *All 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.
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* > *All Chassis* and in the content pane select the name of a chassis in the list. In the lower content pane, select the *PEM* tab.

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

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 (FG-5140 and FG-5140B chassis only)

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

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* > *All Chassis* and in the content pane select the name of a chassis in the list. In the navigation pane, select the *Shelf Manager* item.

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. *OK* indicates that all monitored voltages are within acceptable ranges. *Below lower critical* indicates that a monitored voltage is too low.
Voltage	Voltage value for a voltage sensor.
Edit 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* > *All Chassis* and in the content pane select the name of a chassis in the list. In the navigation pane, select the *SAP* item.

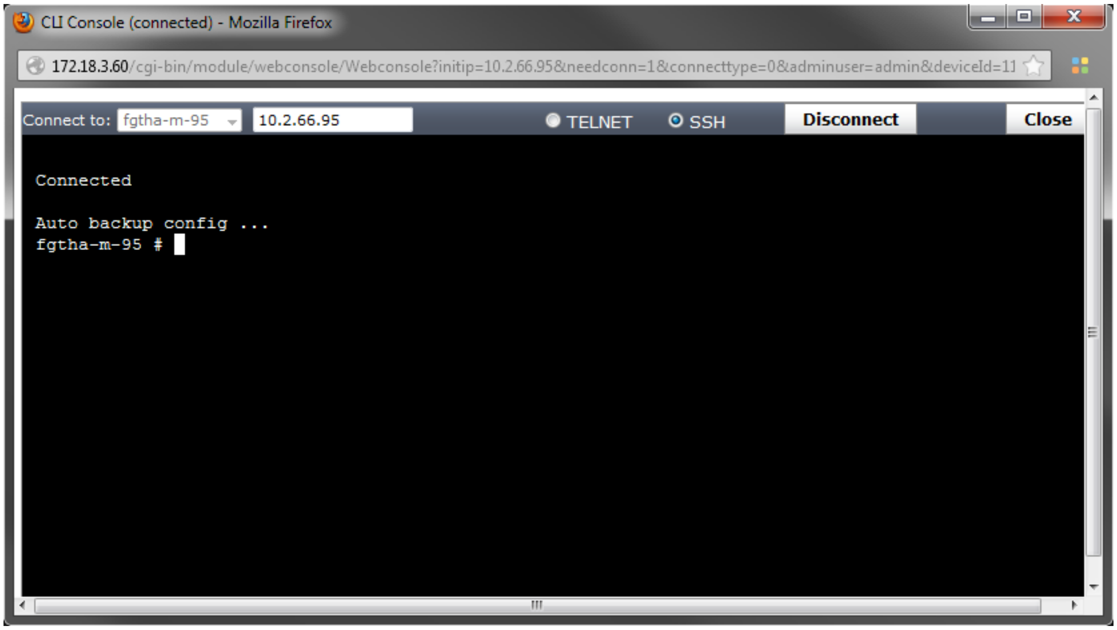
Presence	Indicates if the SAP is present or absent.
Telco Alarm	Telco form-c relay connections for minor, major and critical power faults provided by the external dry relay Telco alarm interface (48VDC).
Air Filter	Indicates if the air filter is present or absent.
Model	The SAP model.
State	The operation 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.

Using the CLI console for managed devices

You can access the CLI console of the managed devices. In the *Device Manager* dashboard, select *Connect to CLI via* on the *Connection Summary* widget. You can select to connect via Telnet or SSH.

Figure 94:CLI console


CLI Console (connected) - Mozilla Firefox
172.18.3.60/cgi-bin/module/webconsole/Webconsole?initip=10.2.66.95&needconn=1&connecttype=0&adminuser=admin&deviceId=11
Connect to: fgtha-m-95
10.2.66.95
○ TELNET
● SSH
Disconnect
Close

```
Connected

Auto backup config ...
fgtha-m-95 #
```

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

You can cut (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*.

FortiManager Wizards

The FortiManager *Device Manager* tab provides you with device and installation wizards to aid you in various administrative and maintenance tasks. Using these tools can help you shorten the amount of time it takes to do many common tasks.

FortiManager v5.0 offers four wizards:

- *Add Device* wizard
  - *Discover*

    The device will be probed using the provided IP address and credentials to determine the model type and other important information.
  - *Add Model Device*

    The device will be added using the chosen model type and other explicitly entered information.
- *Install* wizard
  - *Install Policy Package & Device Settings*

    Install a specific policy package. Any device specific settings for devices associated with the package will also be installed.
  - *Install Device Settings (only)*

    Install only device settings for a selected set of devices; policy and object changes will not be updated from the last install.
- *Import Policy* wizard
  - Import device
- *Quick Instal*l
  - *Re-install Policy Package*

    You can right-click on the *Config Status* column icon to perform a quick install of a policy package without launching the *Install wizard*.

This section will describe each wizard and their usage.

Additional configuration options and short-cuts are available using the right-click menu. Right-click the mouse on different navigation panes on the Web-based Manager page to access these options.

Add device wizard

The *Add Device* wizard allows you to discover, add or import devices to you FortiManager unit.

The *Import Device* function allows you to quickly and easily import all the policies and their dependent objects from a device into the policy database of your FortiManager unit. The import wizard will also perform multiple checks on the items being imported to check for potential problems or conflicts.

The *Add Model Device* function allows you to quickly and easily add devices to be centrally managed by your FortiManager unit.

A shortened version of the *Add Device* wizard can also be used to import policies to an already installed or imported device. See "Import policy wizard" on page 185.

Launching the add device wizard

To launch the Add Device wizard:

- If ADOMs are enabled, right-click on the *Device Manager* tree-menu or right content pane, select *Add Device*.
- If ADOMs are not enabled, select *Add Device* from the *Device Manager* toolbar.

The *Add Device* wizard opens.

Use the *Fast Forward Support* feature to ignore prompts when adding or importing a device. The wizard will only stop if there are errors with adding a device or importing policies or objects from a device or VDOM.

Add device wizard options

Select *Discover* for devices which are currently online and discoverable on your network. Select *Add Model Device* to provision a device, which is not yet online, on the FortiManager.

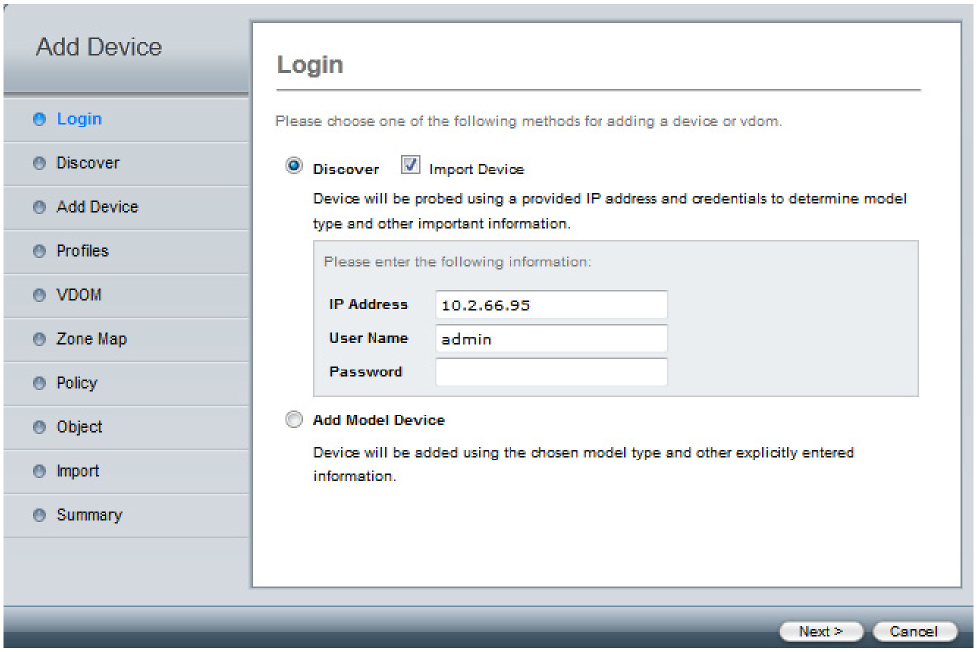
Discover

You will require the IP address of the unit you wish to add, as well as the unit's login and password. The device is probed using the provided IP address and credentials to determine model type and other important information. See "Adding a device" on page 130.

Import device

This option allows you to import a device and bring all of its policies and objects into the FortiManager system. You will require the IP address of the unit you wish to import, as well as the unit's login and password. Select *Import Device* to use this method. See "To add a device using Add Device wizard (Discovery mode):" on page 161.

Figure 95: Discover mode



Login

Please choose one of the following methods for adding a device or vdom.

● Discover ☑ Import Device

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

Please enter the following information:

IP Address	10.2.66.95
User Name	admin
Password	

○ Add Model Device

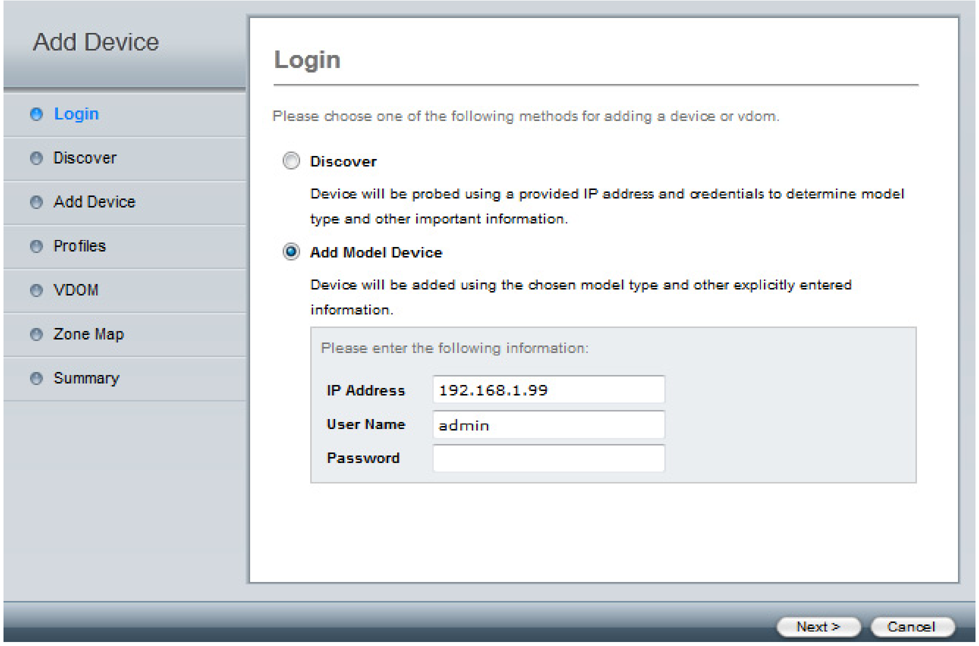
Device will be added using the chosen model type and other explicitly entered information.

Discover	Device will be probed using a provided IP address and credentials to determine model type and other important information.
Import Device	Select to Import device policies and objects.
IP Address	Enter the device IP address. This IP will be probed to complete the import.
User Name	Enter the user name for the device.
Password	Enter the password for the device.

Add model device

If you have a new unit you wish to install, but it is not yet online, you can use this feature to add it to your FortiManager. You must have all related information about the unit to use this feature. See “Adding a device” on page 130.

Figure 96: Add model device mode



Login

Please choose one of the following methods for adding a device or vdom.

○ Discover

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

● Add Model Device

Device will be added using the chosen model type and other explicitly entered information.

Please enter the following information:

IP Address: 192.168.1.99
User Name: admin
Password:

Add Model Device	Device will be added using the chosen model type and other explicitly entered information.
IP Address	Enter the device IP address. This IP address can be changed if the IP address changes at the time of installation.
User Name	Enter the user name for the device.
Password	Enter the password for the device. (optional)

Add a device using the add device wizard (Discovery mode)

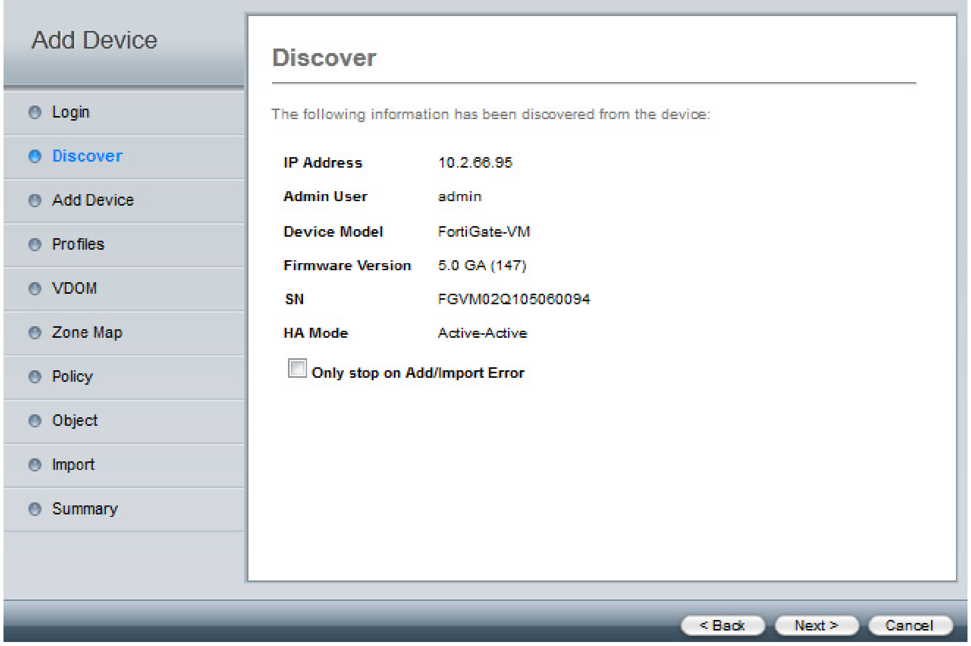
The following steps will guide you through the *Add Device* wizard phases to add a device using *Discovery* mode.

To add a device using Add Device wizard (Discovery mode):

1. Launch the *Add Device* wizard.
2. Select *Discover*, and enable *Import Device* on the *Login* phase page.
3. Enter the IP address, user name and password for the device, and select *Next*.

4. The FortiManager will probe the IP address on your network to discover device details including the following:
   - IP address
   - Administrative user name
   - Device model
   - Firmware version (build)
   - Serial number
   - High Availability mode

Figure 97: Discover phase



Discover

The following information has been discovered from the device:

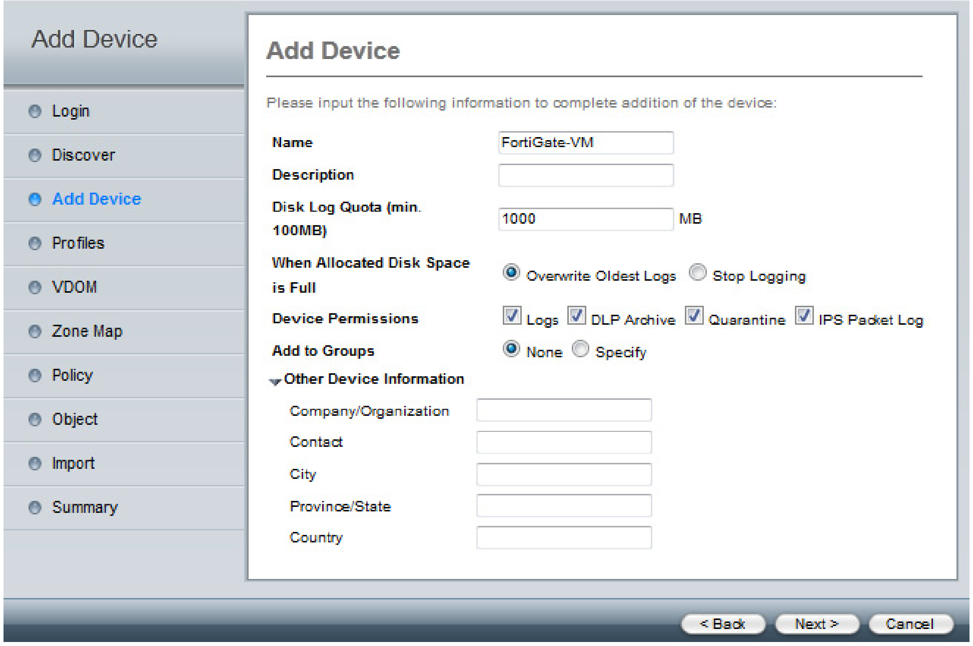
IP Address	10.2.66.95
Admin User	admin
Device Model	FortiGate-VM
Firmware Version	5.0 GA (147)
SN	FGVM02Q105060094
HA Mode	Active-Active

☐ **Only stop on Add/Import Error**

Only stop on Add/Import Error	Enable the option *Only stop on Add/Import Error*, if you would like the wizard to stop when encountering this error.

5. Select *Next* to continue.
6. Enter the following information:
   - Name
   - Description
   - Disk log quota
   - Behavior when disk is full
   - Device permissions
   - Group information
   - Device contact information

Figure 98: Add device phase



Add Device

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

Name	FortiGate-VM
Description	
Disk Log Quota (min. 100MB)	1000 MB
When Allocated Disk Space is Full	● Overwrite Oldest Logs ○ Stop Logging
Device Permissions	☑ Logs ☑ DLP Archive ☑ Quarantine ☑ IPS Packet Log
Add to Groups	● None ○ Specify
Other Device Information	
Company/Organization	
Contact	
City	
Province/State	
Country	

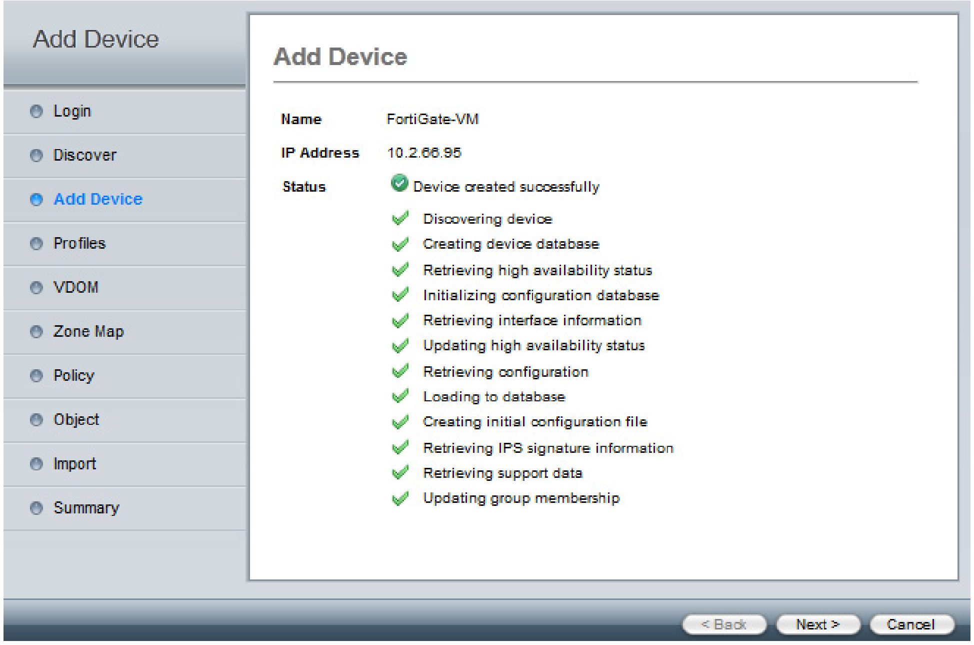
Name	Enter a name for the device.
Description	Enter a description of the device (optional).
Disk Log Quota	Enter a value for the disk log quota in MB.
When Allocated Disk Space is Full	Specify what action to take when the disk space is full: • Overwrite oldest logs • Stop logging
Device Permissions	Specify device permissions: • Logs • DLP Archive • Quarantine • IPS Packet Log
Add to Groups	Select to add the device to any predefined groups.
Other Device Information	Enter other device information (optional), including: • Company/Organization • Contact • City • Province/State • Country

7. Select *Next*.

   The wizard will proceed to discover the device, and perform the following checks:

   - Discovering device
   - Creating device database
   - Retrieving high availability status
   - Initializing configuration database
   - Retrieving interface information
   - Updating high availability status
   - Retrieving configuration
   - Loading to database
   - Creating initial configuration file
   - Retrieving IPS signature information
   - Retrieving support data
   - Updating group membership

Figure 99: Device created successfully



Add Device

Name FortiGate-VM

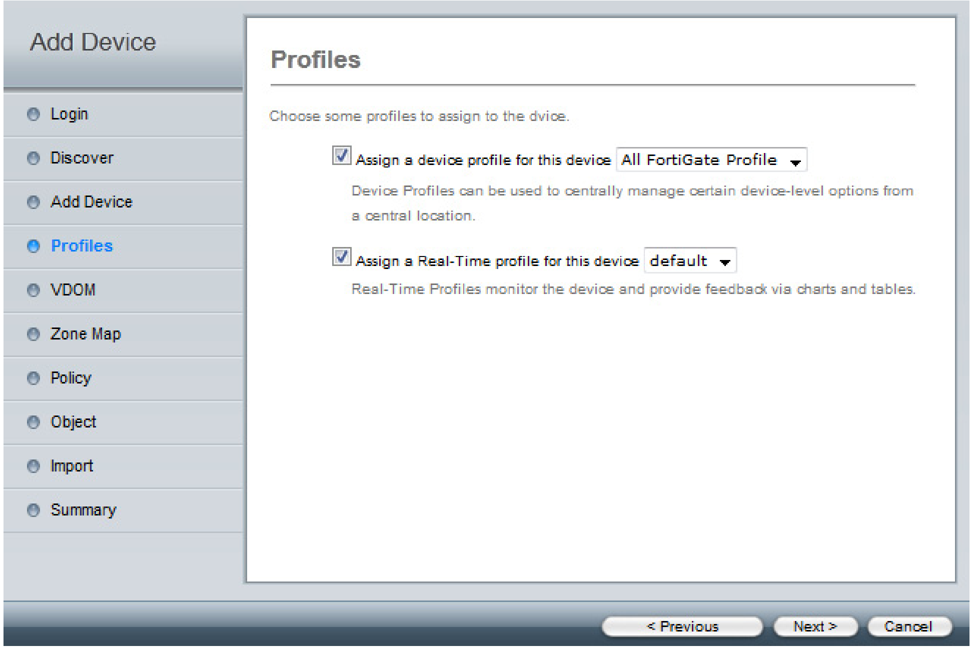
IP Address 10.2.66.95

Status ✓ Device created successfully

✓ Discovering device
✓ Creating device database
✓ Retrieving high availability status
✓ Initializing configuration database
✓ Retrieving interface information
✓ Updating high availability status
✓ Retrieving configuration
✓ Loading to database
✓ Creating initial configuration file
✓ Retrieving IPS signature information
✓ Retrieving support data
✓ Updating group membership

8. Device profiles can be used to centrally manage certain device-level options from a central location. You can assign a device profile using the drop-down menu. Alternatively, you can select to configure all settings per-device inside *Device Manager*.

Figure 100: Device profile phase



Profiles

Choose some profiles to assign to the dvice.

☑ Assign a device profile for this device All FortiGate Profile

Device Profiles can be used to centrally manage certain device-level options from a central location.

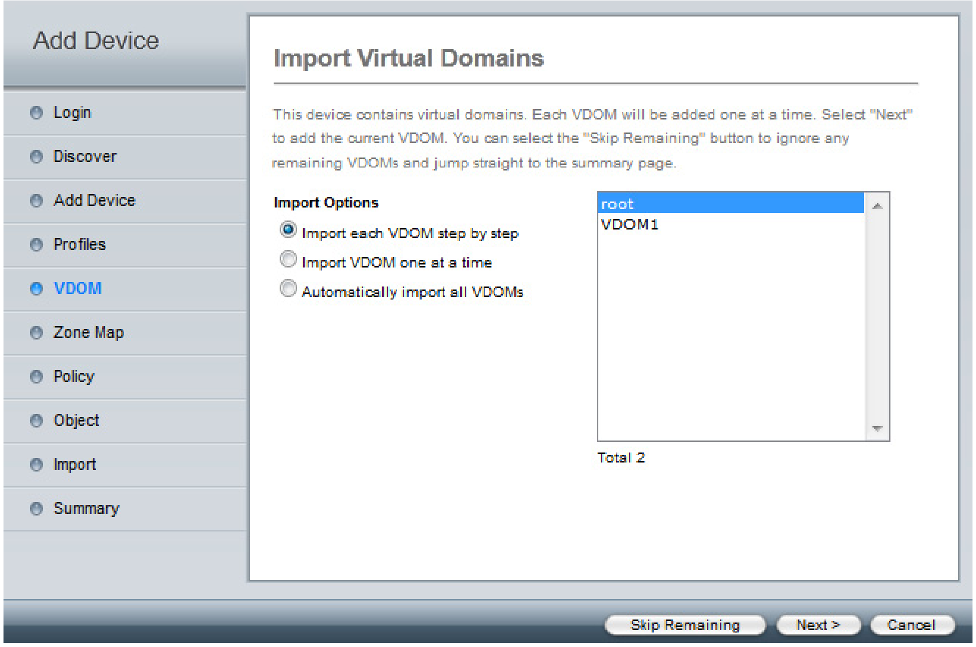
☑ Assign a Real-Time profile for this device default

Real-Time Profiles monitor the device and provide feedback via charts and tables.

Assign a device profile for this device	Device profiles can be used to centrally manage certain device-level options from a central location. Select the check box and select a profile from the drop-down list.
Assign a Real Time profile for this device	Real-time profiles monitor the device and provide feedback via charts and tables. Select the check box and select a profile from the drop-down list.

9. Select *Next* to continue.
10. If VDOMs are not enabled on the device, the wizard will skip the VDOM phase. You can Select to import each VDOM step by step, one at a time, or automatically import all VDOMs.

Figure 101: Import virtual domains phase



Import Virtual Domains

This device contains virtual domains. Each VDOM will be added one at a time. Select "Next" to add the current VDOM. You can select the "Skip Remaining" button to ignore any remaining VDOMs and jump straight to the summary page.

Import Options

● Import each VDOM step by step

○ Import VDOM one at a time

○ Automatically import all VDOMs

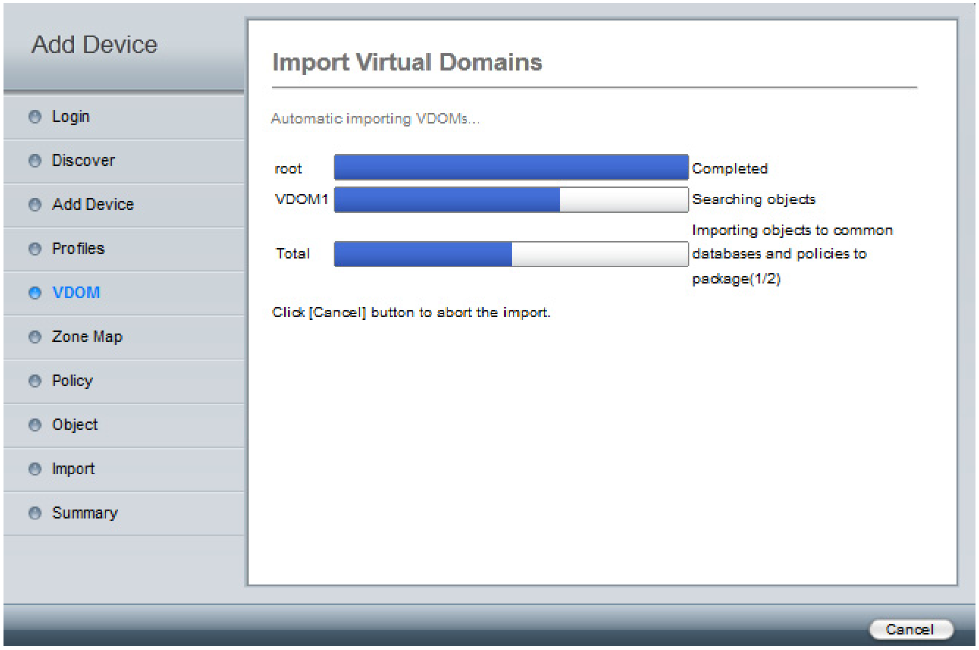
root
VDOM1

Total 2

Import Options The wizard will detect if the device contains virtual domains (VDOMs). You can select the behavior for FortiManager to take to import these VDOMs. Import options include:

- Import each VDOM step by step
- Import VDOM one at a time
- Automatically import all VDOMs

Table 11: Import Virtual Domains phase



Import Virtual Domains

Automatic importing VDOMs...

root Completed

VDOM1 Searching objects

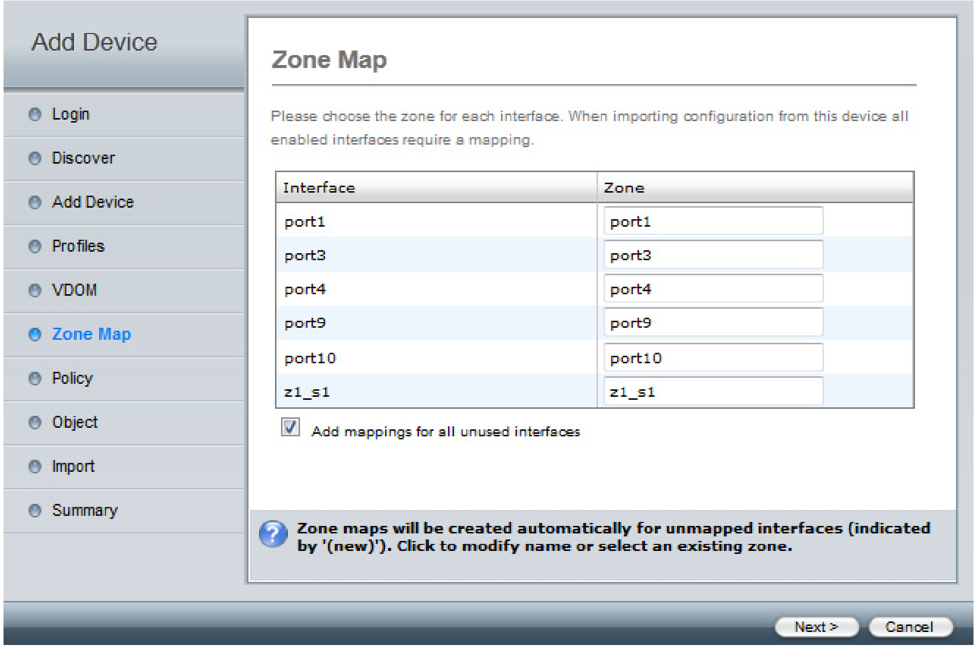
Total Importing objects to common databases and policies to package(1/2)

Click [Cancel] button to abort the import.

11. You can use the global zone map section of the wizard to map your dynamic interface zones.

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

Figure 102: Zone map phase



Zone Map

Please choose the zone for each interface. When importing configuration from this device all enabled interfaces require a mapping.

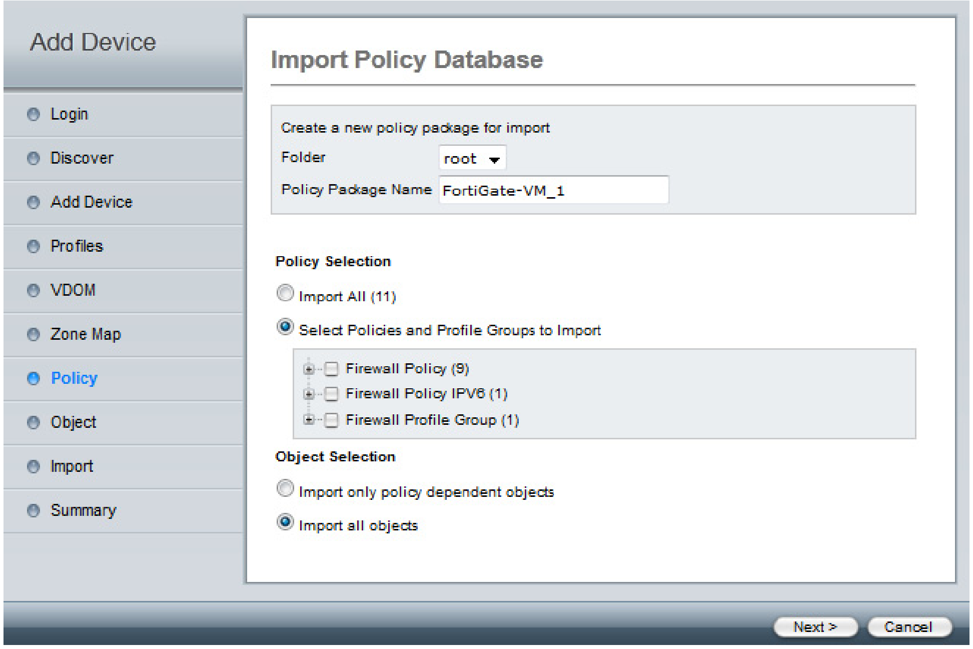
Interface	Zone
port1	port1
port3	port3
port4	port4
port9	port9
port10	port10
z1_s1	z1_s1

☑ Add mappings for all unused interfaces

Zone maps will be created automatically for unmapped interfaces (indicated by '(new)'). Click to modify name or select an existing zone.

12. Select *Next* to continue. The wizard will then perform a policy search to find all policies in preparation for importation into FortiManager's database. Once this step is complete, you will be shown a summary of the policies. Choose a folder on the drop-down list, enter a new policy package name, and select the policies you would like to import from the list. You can also select to import only policy dependent objects or import all objects.

Figure 103: Import policy database phase



Import Policy Database

Create a new policy package for import

Folder: root

Policy Package Name: FortiGate-VM_1

Policy Selection

○ Import All (11)

● Select Policies and Profile Groups to Import

- □ Firewall Policy (9)
- □ Firewall Policy IPV6 (1)
- □ Firewall Profile Group (1)

Object Selection

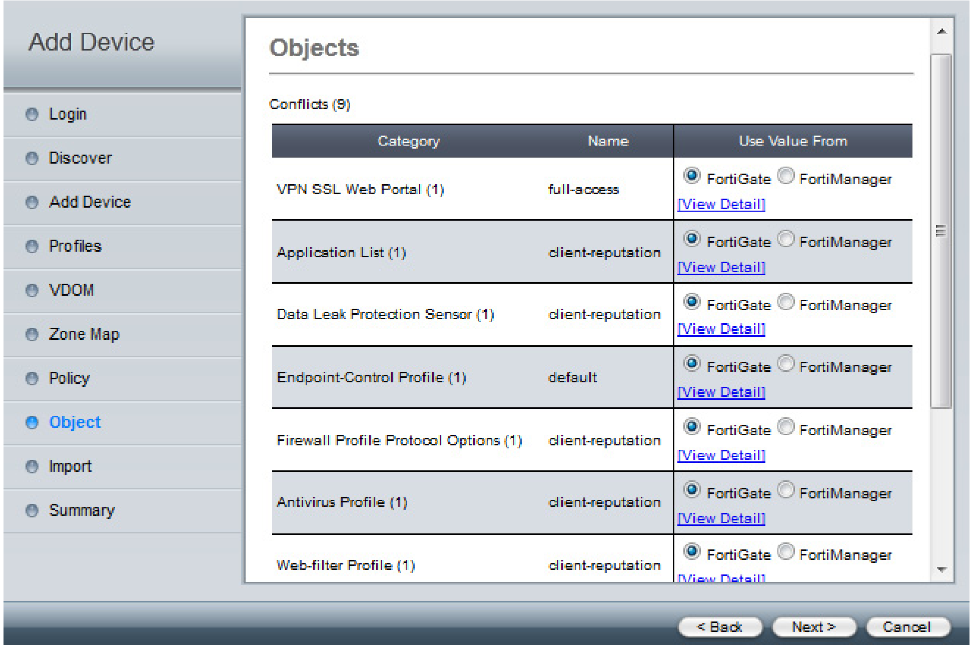
○ Import only policy dependent objects

● Import all objects

Folder	Select the folder using the drop-down list.
Policy Package Name	Enter a *Policy Package Name* (if required).
Policy Selection	
Import All	Select to import all policies.
Select Policies and Profile Groups to Import	Select to import specific policies and profile groups on the tree-menu.
Object Selection	
Import only policy dependent objects	Select to import policy dependent objects only for the device.
Import all objects	Select to import all objects for the selected device.

13. Select *Next* to continue. The wizard then searches the unit for objects to import, and reports any conflicts it detects. If conflicts are detected, you can decide whether to use the FortiGate value or the FortiManager value.

Figure 104: Object phase



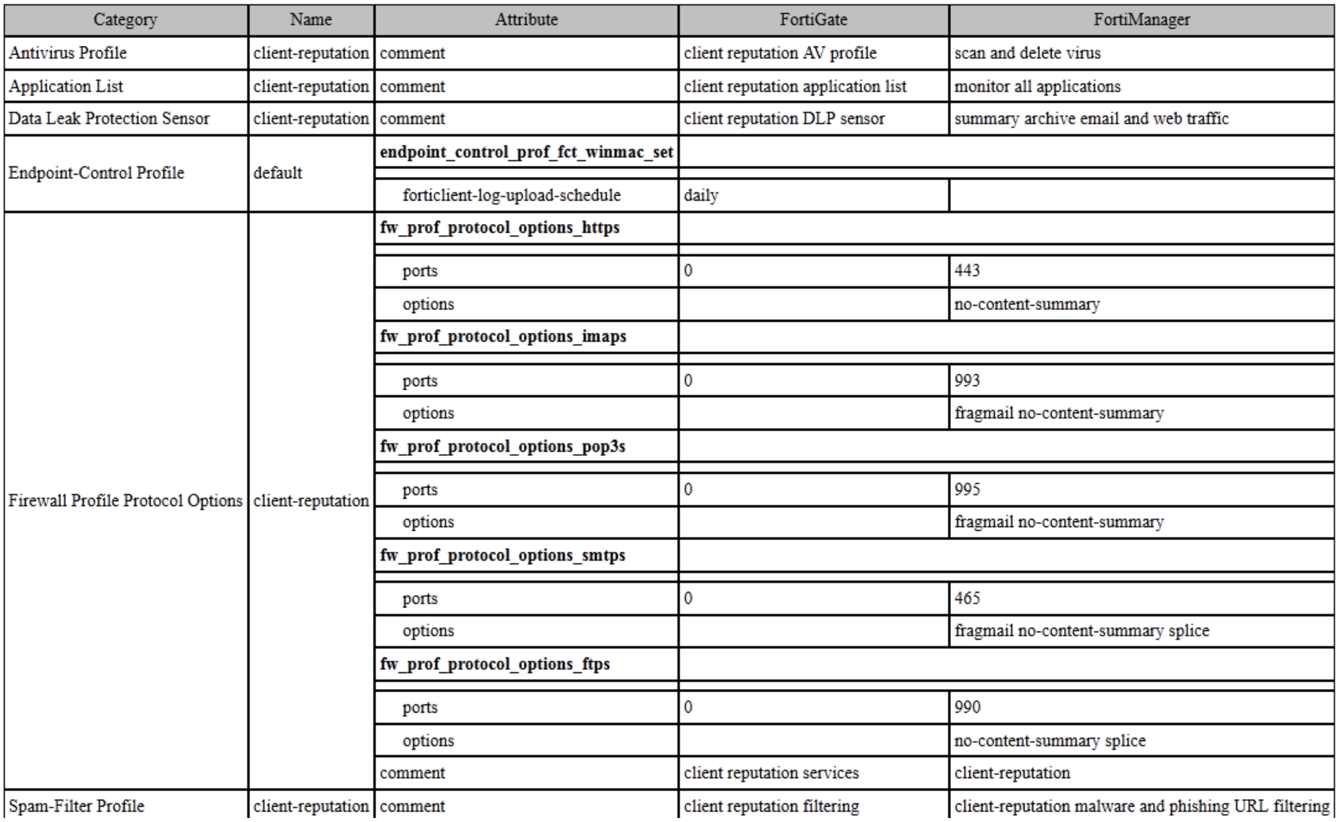
Objects

Conflicts (9)

Category	Name	Use Value From
VPN SSL Web Portal (1)	full-access	● FortiGate ○ FortiManager [View Detail]
Application List (1)	client-reputation	● FortiGate ○ FortiManager [View Detail]
Data Leak Protection Sensor (1)	client-reputation	● FortiGate ○ FortiManager [View Detail]
Endpoint-Control Profile (1)	default	● FortiGate ○ FortiManager [View Detail]
Firewall Profile Protocol Options (1)	client-reputation	● FortiGate ○ FortiManager [View Detail]
Antivirus Profile (1)	client-reputation	● FortiGate ○ FortiManager [View Detail]
Web-filter Profile (1)	client-reputation	● FortiGate ○ FortiManager [View Detail]

14. If conflicts occur, you can scroll down on this page to download the conflict file. This file is HTML-based and provides details of conflicts.

Figure 105: Download conflict file

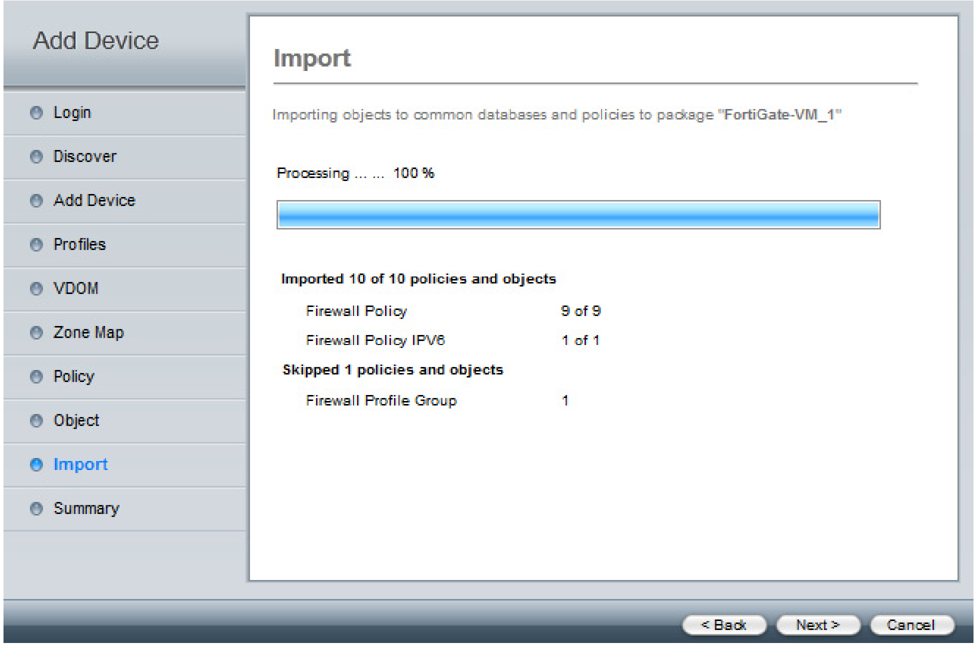


Category	Name	Attribute	FortiGate	FortiManager
Antivirus Profile	client-reputation	comment	client reputation AV profile	scan and delete virus
Application List	client-reputation	comment	client reputation application list	monitor all applications
Data Leak Protection Sensor	client-reputation	comment	client reputation DLP sensor	summary archive email and web traffic
Endpoint-Control Profile	default	**endpoint_control_prof_fct_winmac_set**		
		forticlient-log-upload-schedule	daily	
Firewall Profile Protocol Options	client-reputation	**fw_prof_protocol_options_https**		
		ports	0	443
		options		no-content-summary
		fw_prof_protocol_options_imaps		
		ports	0	993
		options		fragmail no-content-summary
		fw_prof_protocol_options_pop3s		
		ports	0	995
		options		fragmail no-content-summary
		fw_prof_protocol_options_smtps		
		ports	0	465
		options		fragmail no-content-summary splice
		fw_prof_protocol_options_ftps		
		ports	0	990
		options		no-content-summary splice
		comment	client reputation services	client-reputation
Spam-Filter Profile	client-reputation	comment	client reputation filtering	client-reputation malware and phishing URL filtering

15. Select *Next*.

The wizard will import policies and objects into its database.

Figure 106: Import phase



Import

Importing objects to common databases and policies to package "FortiGate-VM_1"

Processing ... ... 100 %

Imported 10 of 10 policies and objects

Firewall Policy	9 of 9
Firewall Policy IPV6	1 of 1

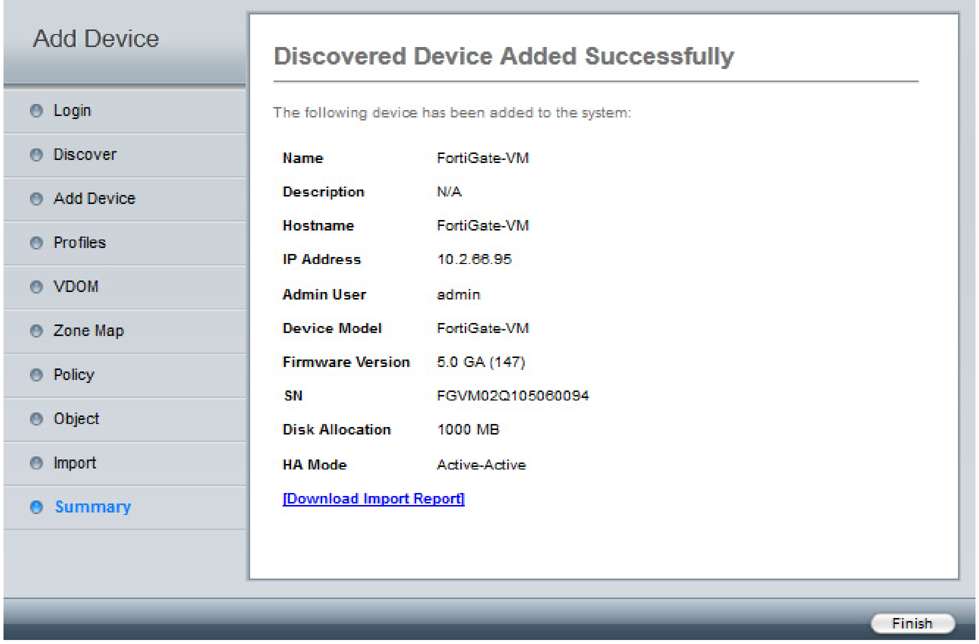
Skipped 1 policies and objects

Firewall Profile Group	1

16. Select *Next*.

The wizard will present a message *Discovered Device Added Successfully* and provides a detailed summary of the import. You can select to download the import report. This report is only available on this page.

Figure 107: Summary phase



Discovered Device Added Successfully

The following device has been added to the system:

Name	FortiGate-VM
Description	N/A
Hostname	FortiGate-VM
IP Address	10.2.66.95
Admin User	admin
Device Model	FortiGate-VM
Firmware Version	5.0 GA (147)
SN	FGVM02Q105060094
Disk Allocation	1000 MB
HA Mode	Active-Active

[Download Import Report]

Figure 108: Import report sample

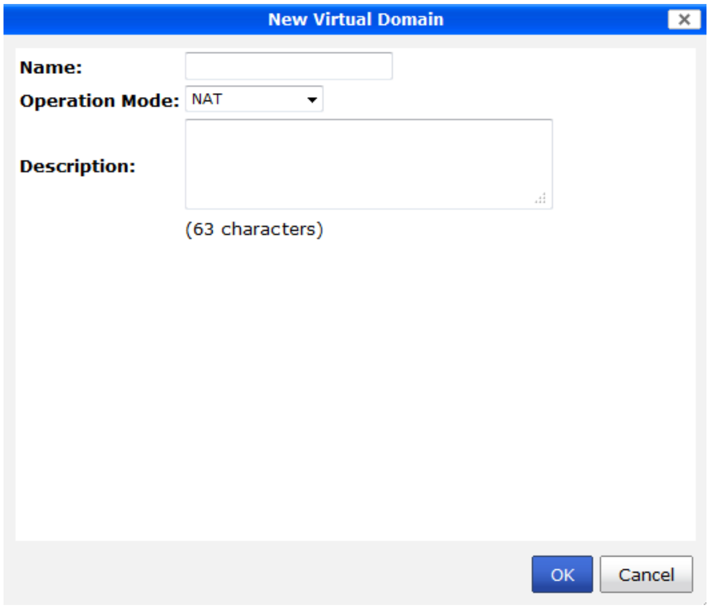
```
Start to import config from device(140) vdom(root) to adom(3)
"firewall schedule recurring",SUCCESS,"(name=always, oid=465,
DUPLICATE)"
"firewall address",SUCCESS,"(name=all, oid=300, DUPLICATE)"
"firewall address",SUCCESS,"(name=ad1, oid=460)"

"firewall addrgrp",SUCCESS,"(name=adgr1, oid=461)"

"firewall ippool",SUCCESS,"(name=pool1, oid=462)"

"firewall central-nat",SUCCESS,"(name=ID:1 (#1), oid=495)"

"firewall profile-protocol-options",SUCCESS,"(name=default, oid=
326)"

"antivirus profile",SUCCESS,"(name=default, oid=433, DUPLICATE)"
"firewall policy",SUCCESS,"(name=ID:1 (#1), oid=493)"
"firewall policy",SUCCESS,"(name=ID:2 (#2), oid=494)"
```

17. Select *Finish* to close the wizard.

Add a VDOM

Right-click on the content pane for a particular device and select *Add VDOM* from the right-click menu to add a VDOM to a managed FortiGate device.

Figure 109: Add a VDOM



New Virtual Domain

Name:

Operation Mode: NAT

Description:

(63 characters)

Name	Enter a name for the new virtual domain.
Operation Mode	Select either NAT or Transparent for operation mode.
Description	Enter a description. (Optional)

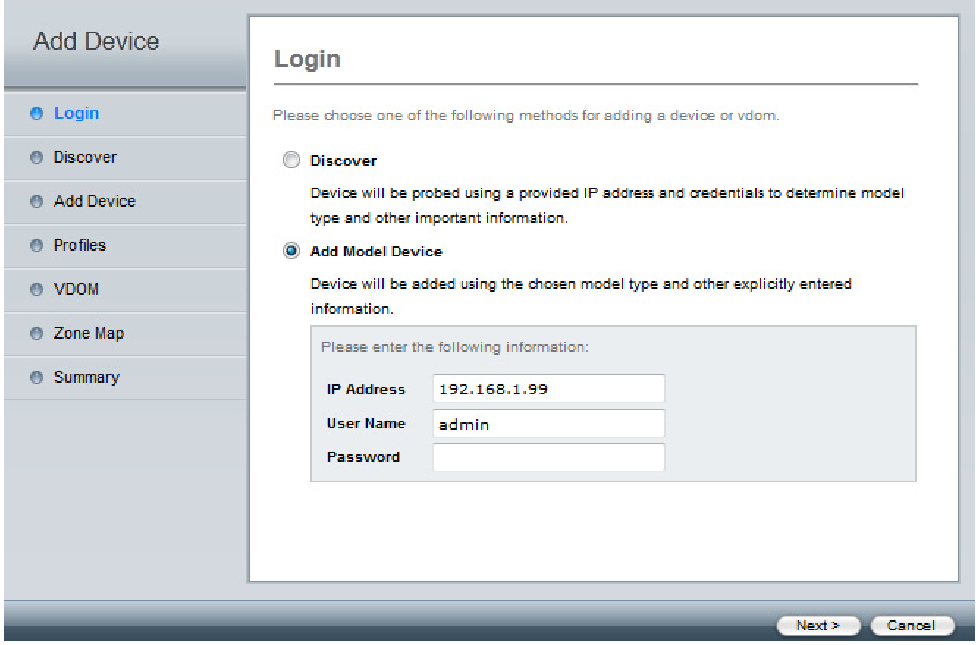
Add a device using the add device wizard (Add model device)

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

To add a model device:

1. Right-click the tree-menu or right content pane to launch the *Add Device* wizard.
2. Select *Add Model Device* on the *Login* phase page.
3. Enter the IP address, user name and password for the device, and select *Next*.

Figure 110: Login phase



Login

Please choose one of the following methods for adding a device or vdom.

○ Discover

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

● Add Model Device

Device will be added using the chosen model type and other explicitly entered information.

Please enter the following information:

IP Address	192.168.1.99
User Name	admin
Password	

Add Model Device	Device will be added using the chosen model type and other explicitly entered information.
IP Address	Enter the device IP address. This IP address can be changed if the IP address changes at the time of installation.
User Name	Enter the user name for the device.
Password	Enter the password for the device. (optional)

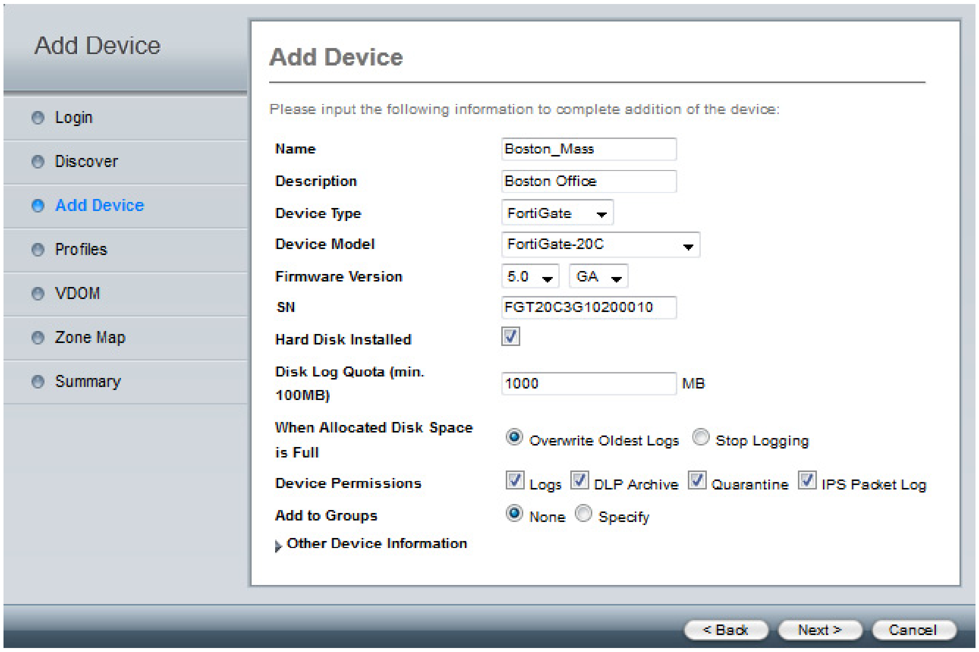
4. Select *Next* to continue
5. Complete the following fields on the *Add Device* phase:

Name	Hard Disk Installed
Description (optional)	Specify if the device has a hard disk installed
Device Type	Disk Log Quota
Device Model	Behavior when disk is full
Firmware Version	Device Permissions

Serial Number	Group information
Enable Interface Mode (select systems)	Other device contact information (optional)

If the device does not support interface mode, the option to enable this feature will not be available.

Figure 111: Add device phase



Add Device

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

Name	Boston_Mass
Description	Boston Office
Device Type	FortiGate
Device Model	FortiGate-20C
Firmware Version	5.0 GA
SN	FGT20C3G10200010
Hard Disk Installed	☑
Disk Log Quota (min. 100MB)	1000 MB
When Allocated Disk Space is Full	● Overwrite Oldest Logs ○ Stop Logging
Device Permissions	☑ Logs ☑ DLP Archive ☑ Quarantine ☑ IPS Packet Log
Add to Groups	● None ○ Specify

▸ Other Device Information

Name	Enter a name for the device.
Description	Enter a description for the device (optional).
Device Type	Select the device type on the drop-down list.
Device Model	Select the device model on the drop-down list.
Firmware Version	Select the firmware version and major release on the drop-down list.
Serial Number	Enter the device serial number. This value must match the device model selected.
Enable Interface Mode	Select to enable interface mode. If the device does not support interface mode, this option is not available.
Hard Disk Installed	This option is available when the device model has a hard disk.
Disk Log Quota.	Enter the disk log quota in MB.
When Allocated Disk Space is Full	Select to overwrite oldest logs or stop logging when the allocated disk space is full.

Device Permissions	Specify device permissions: • Logs • DLP Archive • Quarantine • IPS Packet Log
Add to Groups	Select to add the device to any predefined groups.
Other Device Information	Enter other device information including: • Company/Organization • Contact • City • Province/State • Country

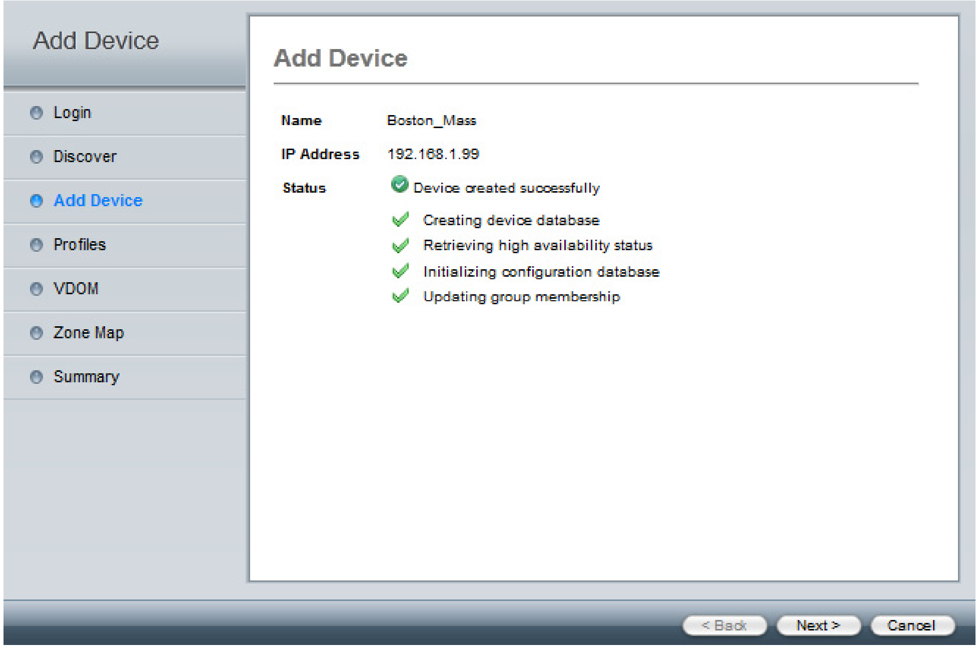
Not all device models are supported in all firmware versions. If you are unable to find the device model under one firmware version, it might be available under a newer version.

Each device must have a unique name, otherwise the wizard will fail.

6. Select *Next*.

   The device will be created in the FortiManager database.

Figure 112: Device created successfully



Add Device

Name Boston_Mass

IP Address 192.168.1.99

Status ✓ Device created successfully

✓ Creating device database

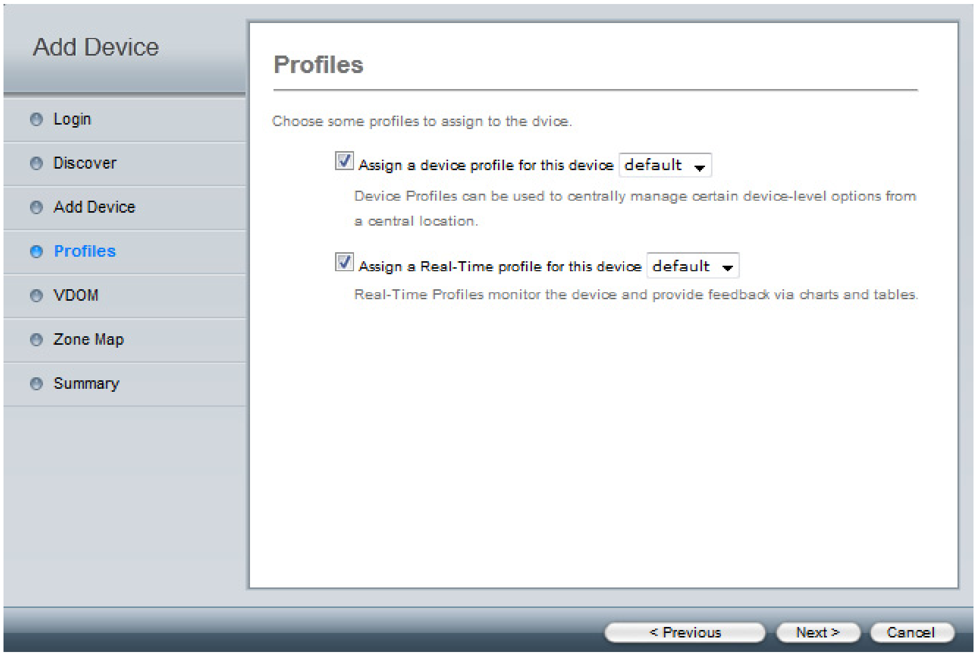
✓ Retrieving high availability status

✓ Initializing configuration database

✓ Updating group membership

7. Device profiles can be used to centrally manage certain device-level options from a central location. You can assign a device profile using the drop-down menu. Alternatively, you can select to configure all settings per-device inside *Device Manager*.

Figure 113: Device profile phase



Profiles

Choose some profiles to assign to the dvice.

☑ Assign a device profile for this device default

Device Profiles can be used to centrally manage certain device-level options from a central location.

☑ Assign a Real-Time profile for this device default

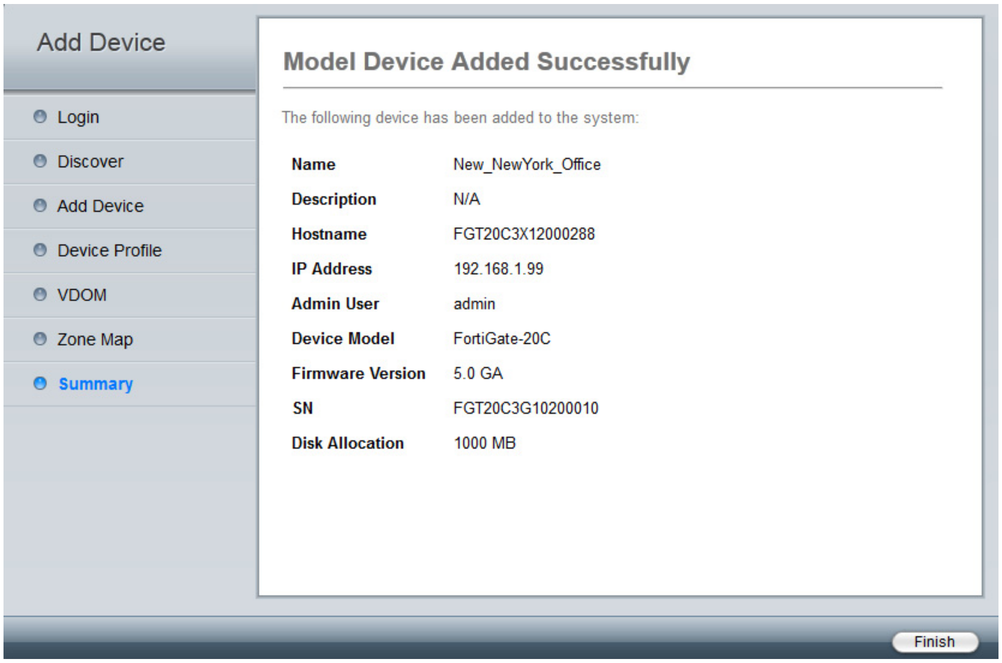
Real-Time Profiles monitor the device and provide feedback via charts and tables.

Assign a device profile for this device	Device profiles can be used to centrally manage certain device-level options from a central location. Select the check box and select a profile from the drop-down list.
Assign a Real Time profile for this device	Real-time profiles monitor the device and provide feedback via charts and tables. Select the check box and select a profile from the drop-down list.

8. Select *Next*.

   The *Add Model Device* wizard proceeds to the summary page.

Figure 114: Summary phase



Model Device Added Successfully

The following device has been added to the system:

Name	New_NewYork_Office
Description	N/A
Hostname	FGT20C3X12000288
IP Address	192.168.1.99
Admin User	admin
Device Model	FortiGate-20C
Firmware Version	5.0 GA
SN	FGT20C3G10200010
Disk Allocation	1000 MB

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

Install wizard

The *Install* wizard will assist you in installing settings to one or more of your FortiGate devices.

Launching the install wizard

To launch the *Install* wizard:

- If ADOMs are enabled, right-click on the *Device Manager* tree-menu or right content pane, select *Install*.
- If ADOMs are not enabled, select *Install* from the *Device Manager* toolbar.

The *Introduction* phase gives you two options for installing settings:

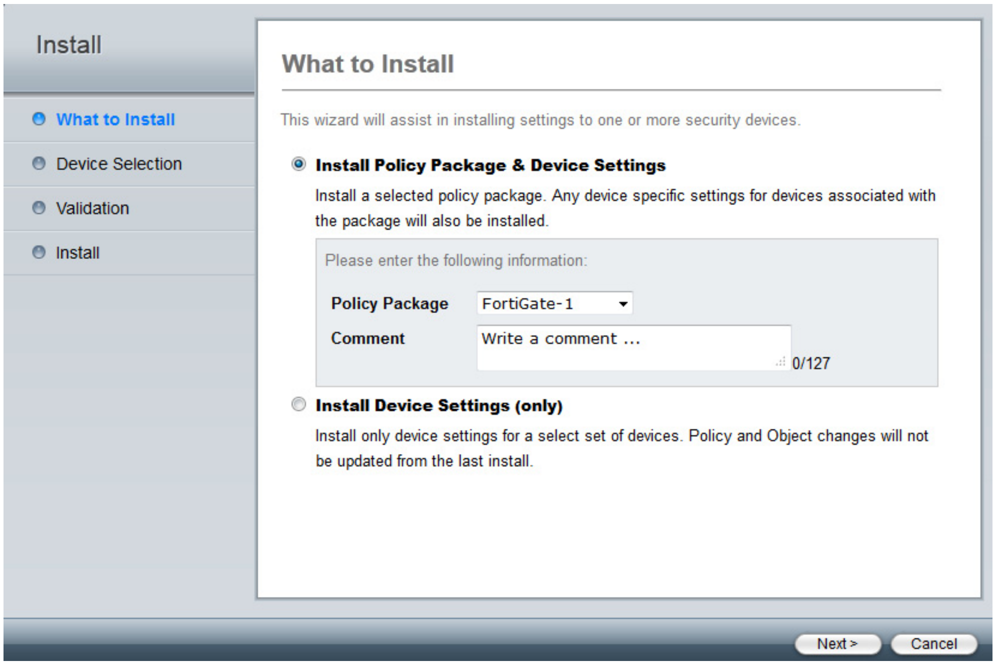
- *Install Policy Package & Device Settings*

  Install a selected policy package. Any device specific settings for devices associated with package will also be included. See "Install policy package and device settings" below.

- *Install Device Settings (only)*

  Install only device settings for a select set of devices. Policy and object changes will not be updated from the last install. See "Installing device settings" on page 181.

Figure 115: Install wizard



What to Install

This wizard will assist in installing settings to one or more security devices.

● **Install Policy Package & Device Settings**

Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Please enter the following information:

Policy Package FortiGate-1

Comment Write a comment ... 0/127

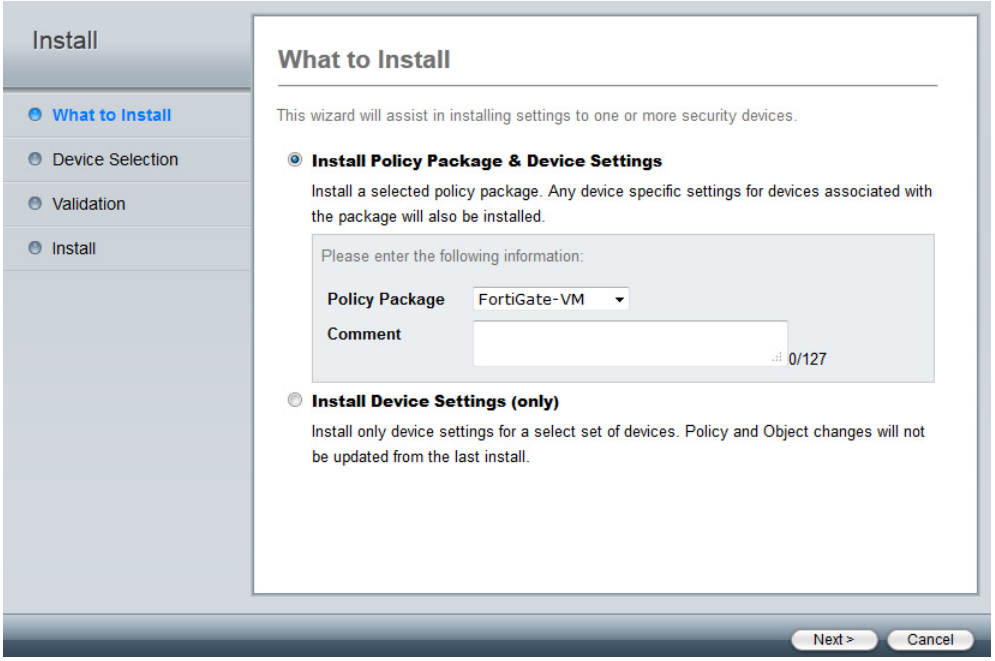
○ **Install Device Settings (only)**

Install only device settings for a select set of devices. Policy and Object changes will not be updated from the last install.

Install policy package and device settings

Select *Install Policy Package & Device Settings*, select the policy package on the drop-down list, and optionally enter a comment for the policy package being installed.

Figure 116: Install policy package and device settings



What to Install

This wizard will assist in installing settings to one or more security devices.

● **Install Policy Package & Device Settings**

Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Please enter the following information:

Policy Package FortiGate-VM

Comment 0/127

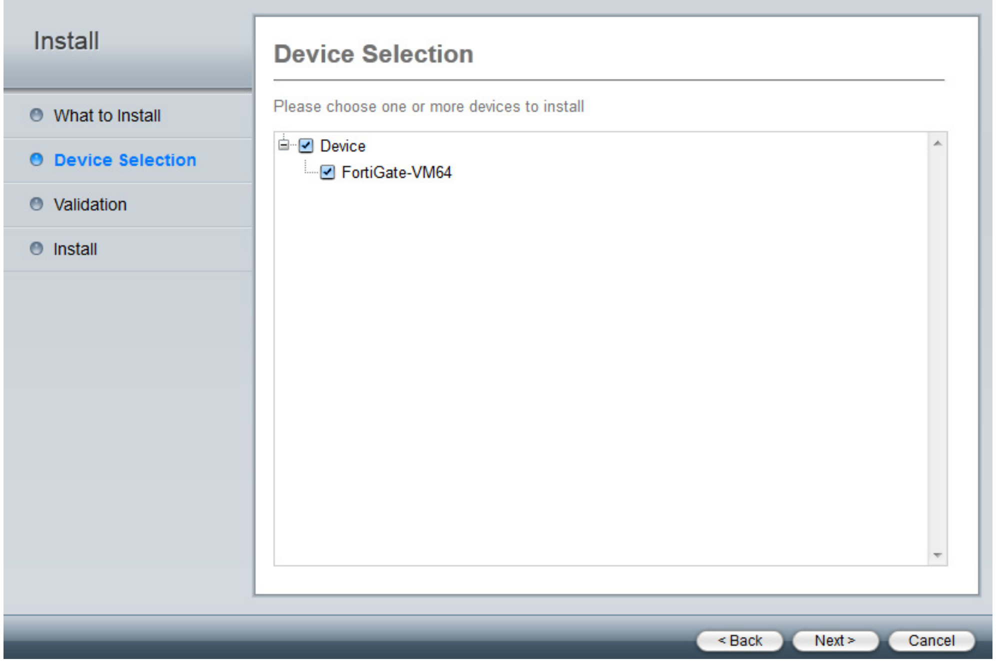
○ **Install Device Settings (only)**

Install only device settings for a select set of devices. Policy and Object changes will not be updated from the last install.

Device selection

The device selection window allows you to choose one or more devices or groups to install.

Figure 117: Device selection phase



Device Selection

Please choose one or more devices to install

☑ Device

☑ FortiGate-VM64

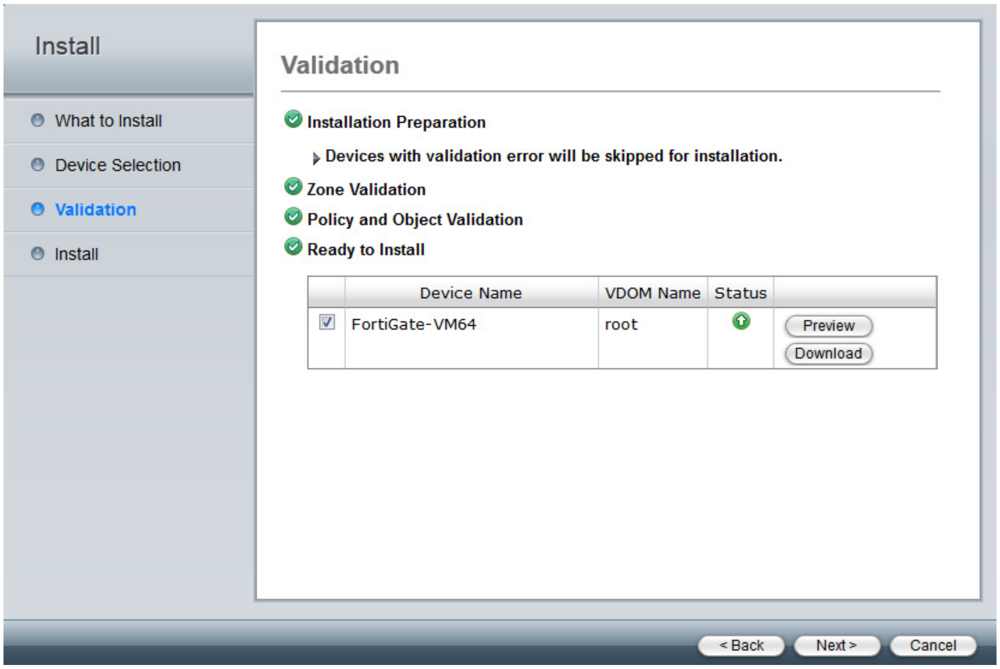
Validation

The *Validation* phase checks the following:

- Installation Preparation
- Zone Validation
- Policy and Object Validation

Devices with a validation error will be skipped for installation.

Figure 118: Validation phase



✓ Installation Preparation

▸ Devices with validation error will be skipped for installation.

✓ Zone Validation

✓ Policy and Object Validation

✓ Ready to Install

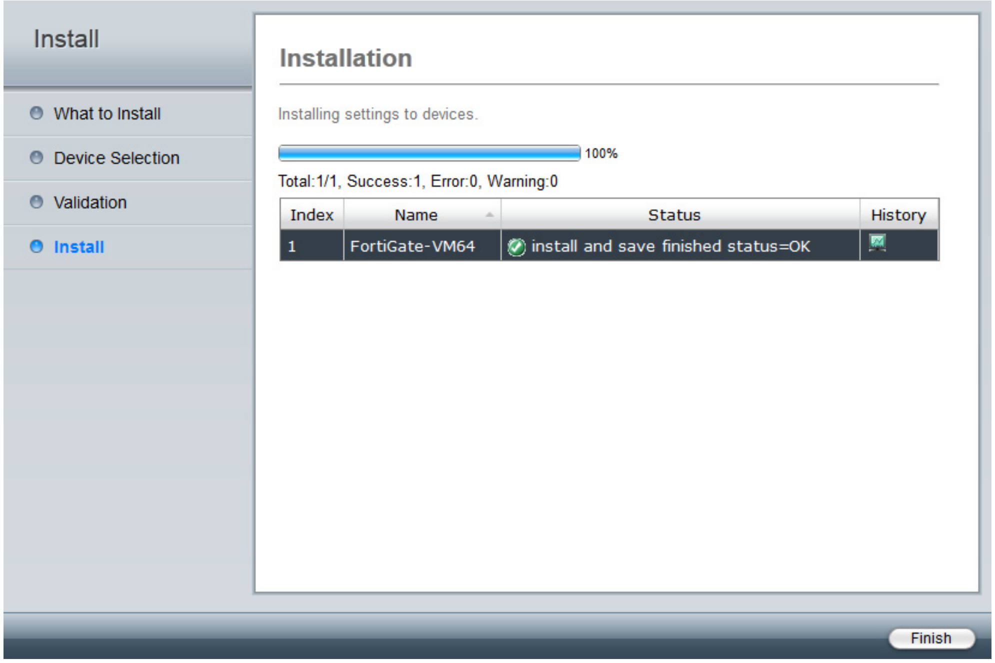
	Device Name	VDOM Name	Status	
☑	FortiGate-VM64	root	⬆	Preview Download

Preview	Select to view device preview.
Download	Select download to open or save the preview file in .txt format.

Installation

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

Figure 119: Policy package installation window



Installation

Installing settings to devices.

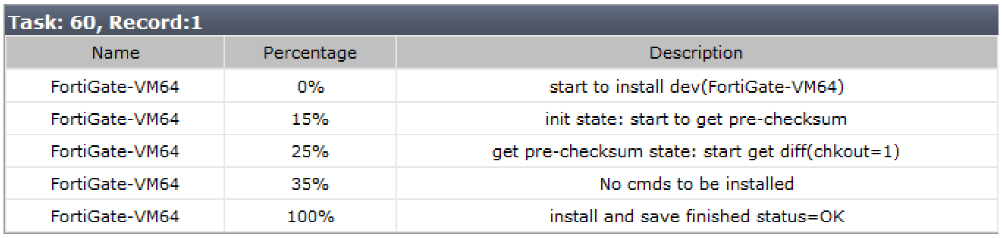
100%

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

Index	Name	Status	History
1	FortiGate-VM64	✓ install and save finished status=OK	

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

Figure 120: Device installation history



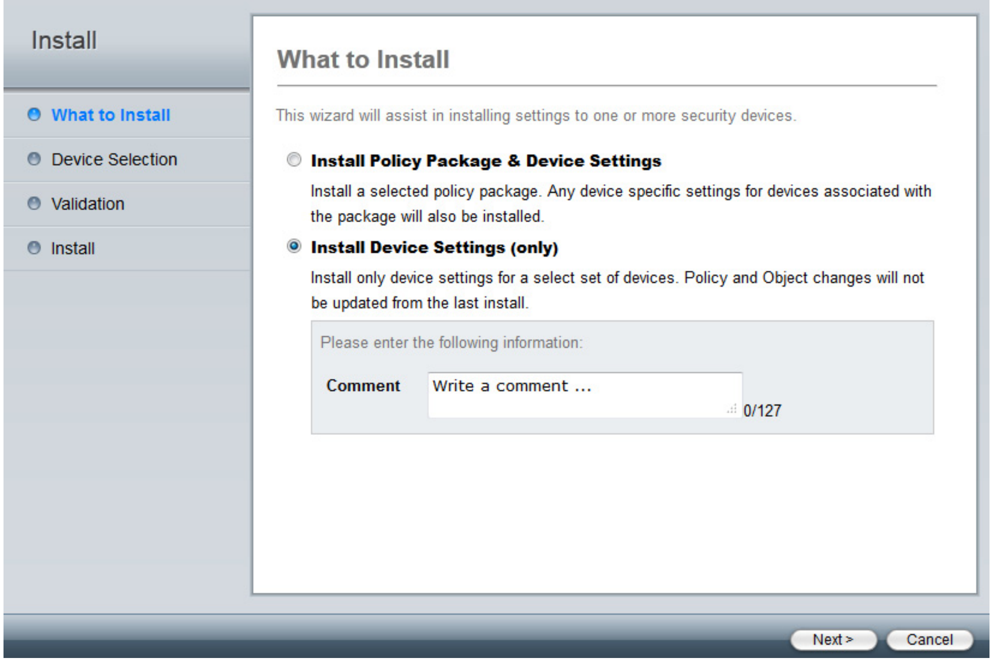
Task: 60, Record:1

Name	Percentage	Description
FortiGate-VM64	0%	start to install dev(FortiGate-VM64)
FortiGate-VM64	15%	init state: start to get pre-checksum
FortiGate-VM64	25%	get pre-checksum state: start get diff(chkout=1)
FortiGate-VM64	35%	No cmds to be installed
FortiGate-VM64	100%	install and save finished status=OK

Installing device settings

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

Figure 121: Install device settings only



What to Install

This wizard will assist in installing settings to one or more security devices.

○ **Install Policy Package & Device Settings**

Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

● **Install Device Settings (only)**

Install only device settings for a select set of devices. Policy and Object changes will not be updated from the last install.

Please enter the following information:

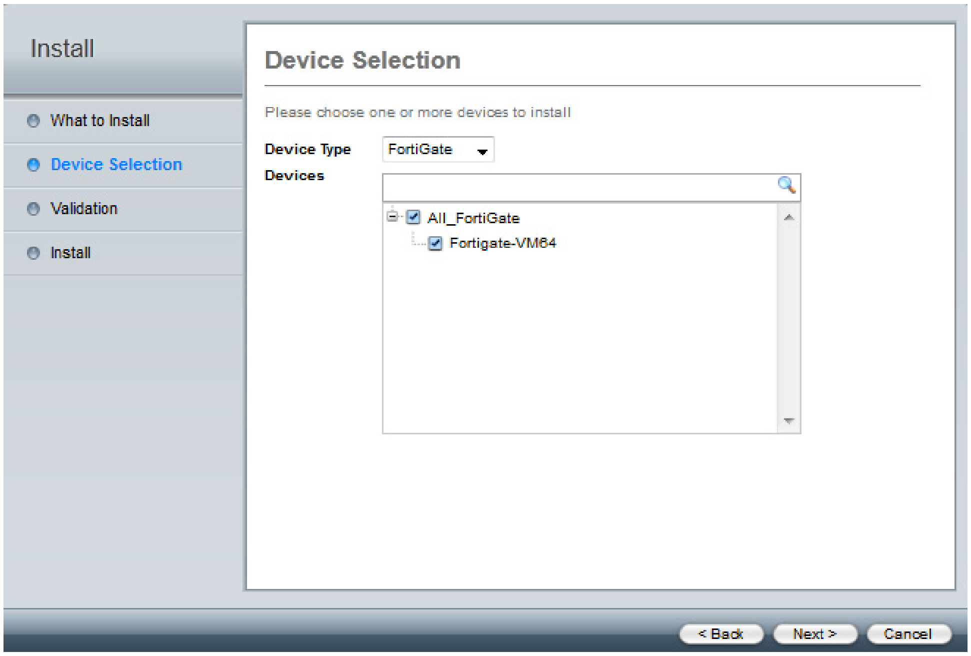
Comment Write a comment ... 0/127

Comment	Enter an option comment.

Device selection

The device selection window allows you to choose the device type and then one or more devices of that type to install.

Figure 122: Device selection window



Please choose one or more devices to install

Device Type: FortiGate

Devices:

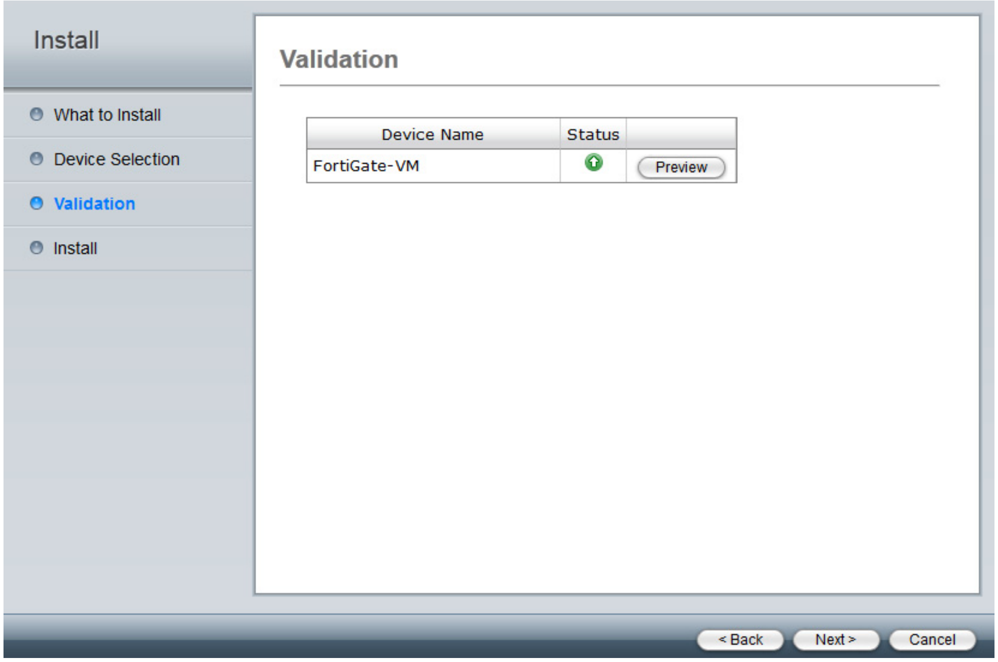
- ☑ All_FortiGate
  - ☑ Fortigate-VM64

Device Selection	Select which devices for installation.

Validation

The validation phase will perform a check on the device and settings to be installed.

Figure 123: Validation phase



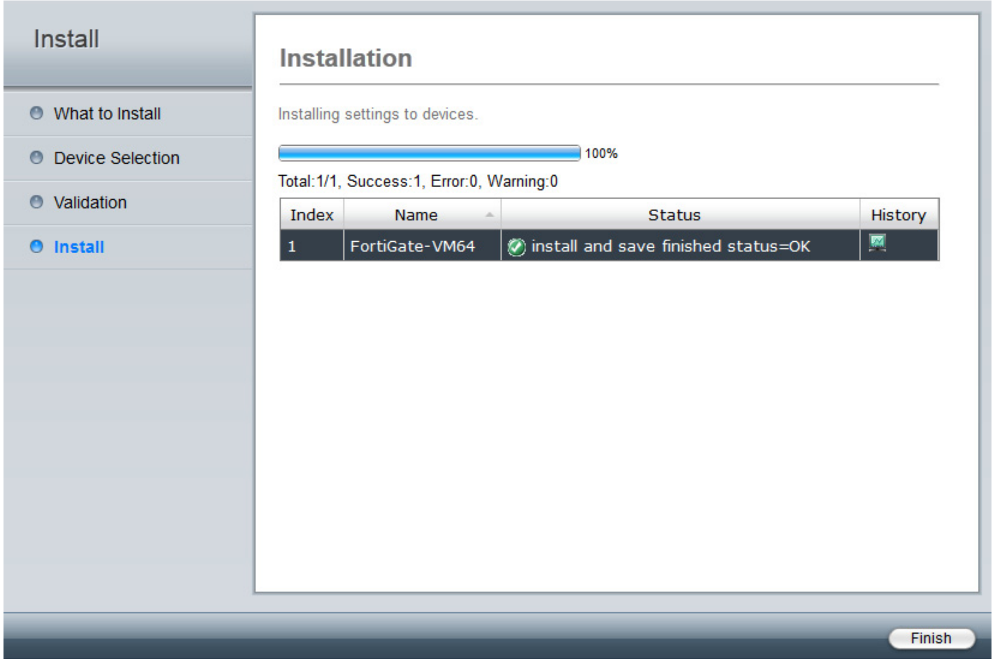
Device Name	Status	
FortiGate-VM	⬆	Preview

Preview	Select to preview installation.
Download	Select download to open or save the preview file in .txt format.

Installation

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

Figure 124: Device settings successful installation window



Installation

Installing settings to devices.

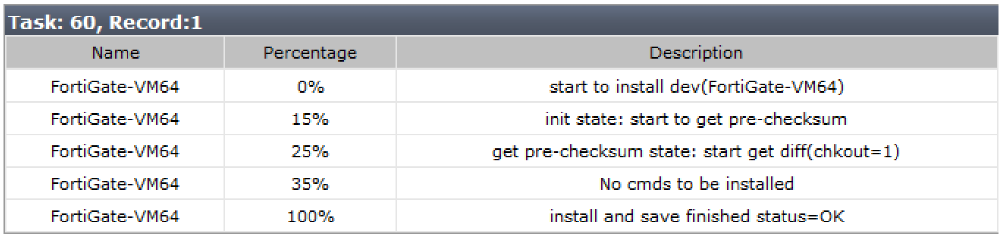
100%

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

Index	Name	Status	History
1	FortiGate-VM64	✓ install and save finished status=OK	

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

Figure 125: Device installation history



Task: 60, Record:1

Name	Percentage	Description
FortiGate-VM64	0%	start to install dev(FortiGate-VM64)
FortiGate-VM64	15%	init state: start to get pre-checksum
FortiGate-VM64	25%	get pre-checksum state: start get diff(chkout=1)
FortiGate-VM64	35%	No cmds to be installed
FortiGate-VM64	100%	install and save finished status=OK

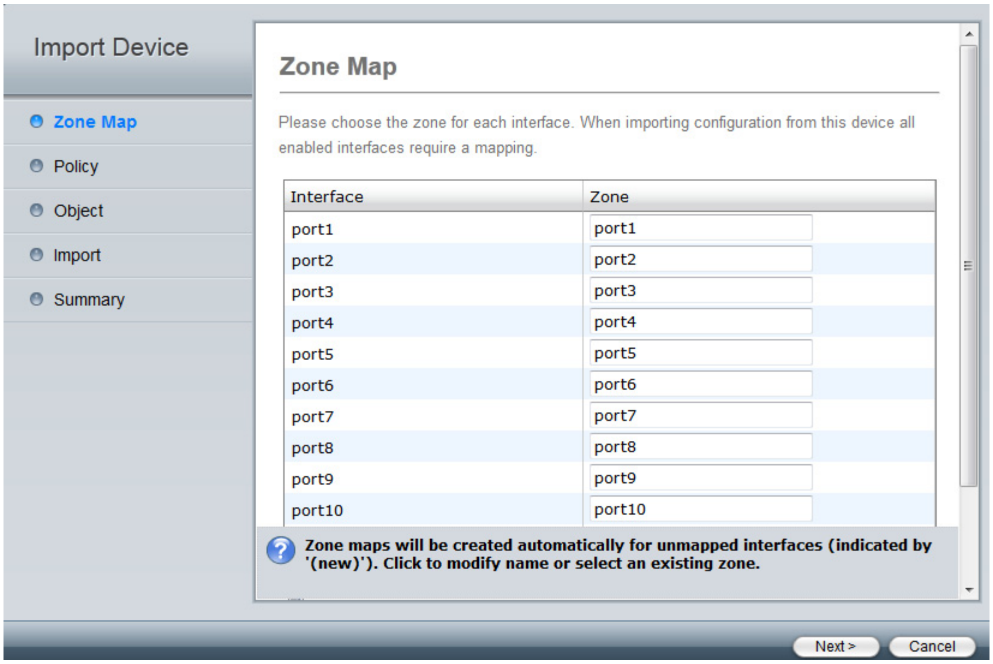
Import policy wizard

You can right-click on the right-content pane and select Import Policy to launch the Import Device wizard. This wizard will allow you to import zone maps, policy database,

Zone map

The Zone Map phase allows you to choose a zone for each interface. When importing configuration from this device all enabled interfaces require a mapping. Zone maps will be created automatically for unmapped interfaces.

Figure 126: Zone map phase



Zone Map

Please choose the zone for each interface. When importing configuration from this device all enabled interfaces require a mapping.

Interface	Zone
port1	port1
port2	port2
port3	port3
port4	port4
port5	port5
port6	port6
port7	port7
port8	port8
port9	port9
port10	port10

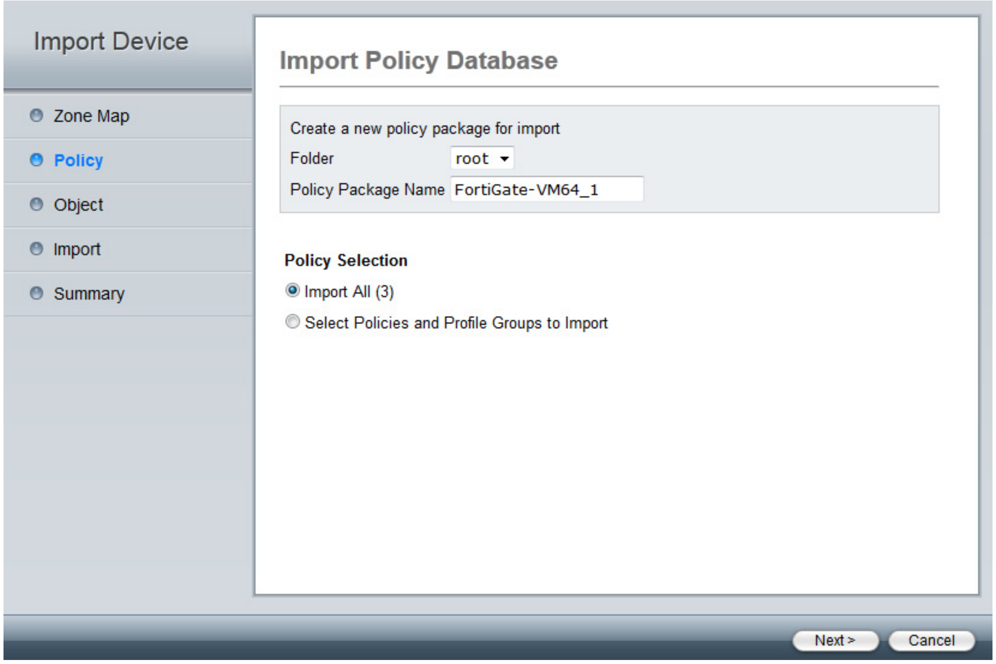
Zone maps will be created automatically for unmapped interfaces (indicated by '(new)'). Click to modify name or select an existing zone.

Add mappings for all unused interfaces	Select to automatically create zone maps for unused interfaces.

Policy

The policy phase allows you to create a new policy package for import. Select the folder on the drop-down menu, and specify the policy package name. You can select to import all policies for select specific policies and profile groups to import.

Figure 127: Policy phase



Create a new policy package for import

Folder: root

Policy Package Name: FortiGate-VM64_1

Policy Selection

● Import All (3)

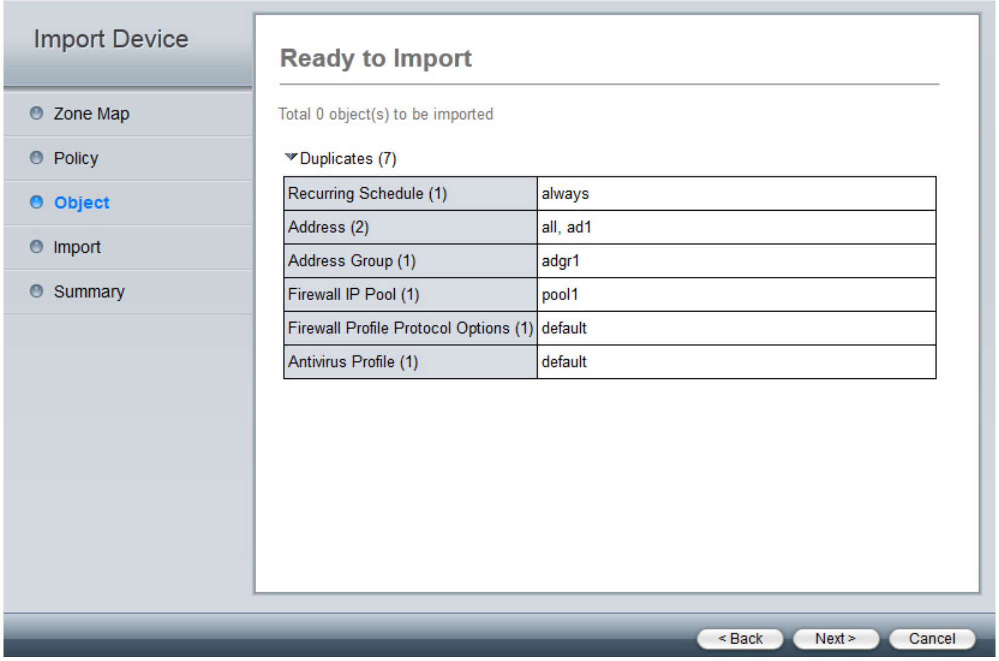
○ Select Policies and Profile Groups to Import

Folder	Select a folder on the drop-down menu.
Policy Package Name	Enter a name for the policy package.
Policy Selection	Select to import all, or select specific policies and policies groups to import.

Object

The object phase will search for dependencies. Duplicates will not be imported.

Figure 128: Object phase



Ready to Import

Total 0 object(s) to be imported

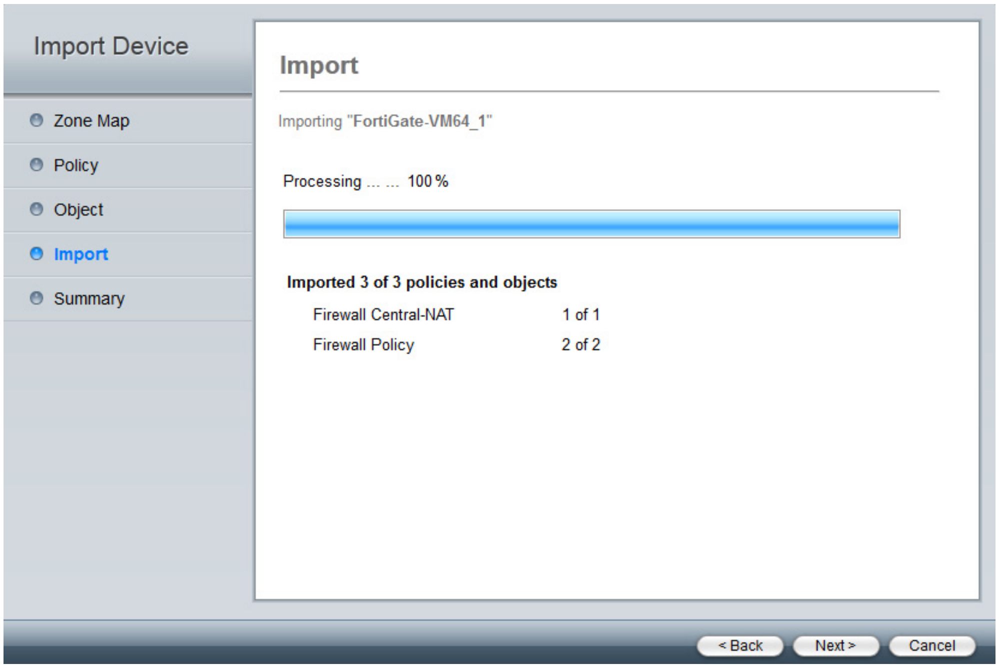
Duplicates (7)

Recurring Schedule (1)	always
Address (2)	all, ad1
Address Group (1)	adgr1
Firewall IP Pool (1)	pool1
Firewall Profile Protocol Options (1)	default
Antivirus Profile (1)	default

Import

The import phase will import zone map, policies, and objects into the FortiManager database.

Figure 129: Import phase



Import

Importing "FortiGate-VM64_1"

Processing ... ... 100 %

Imported 3 of 3 policies and objects

Firewall Central-NAT	1 of 1
Firewall Policy	2 of 2

Summary

The summary phase allows you to download and view the import device summary results.

Figure 130: Summary phase

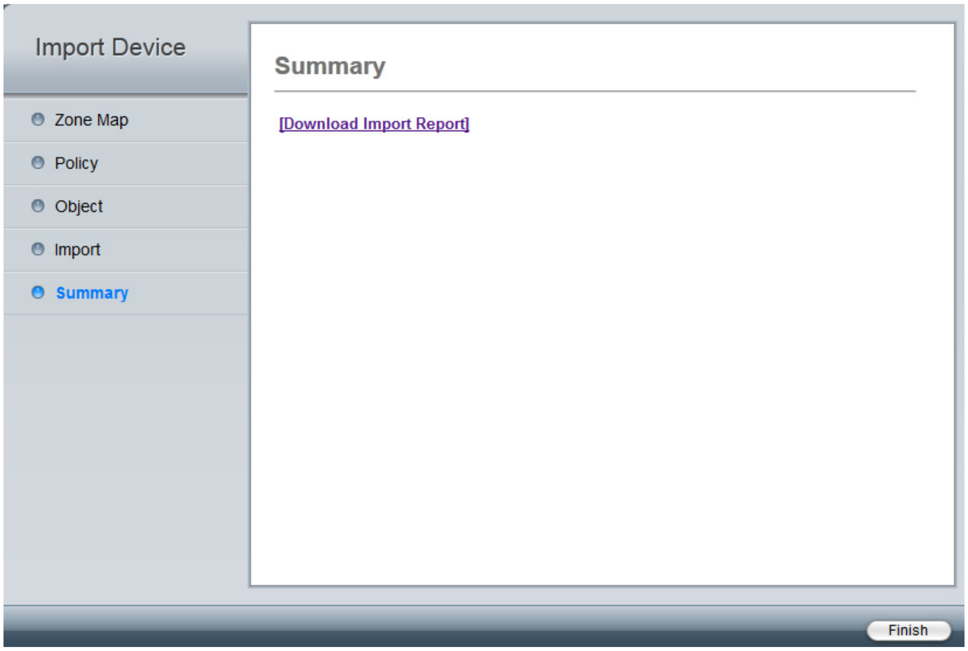
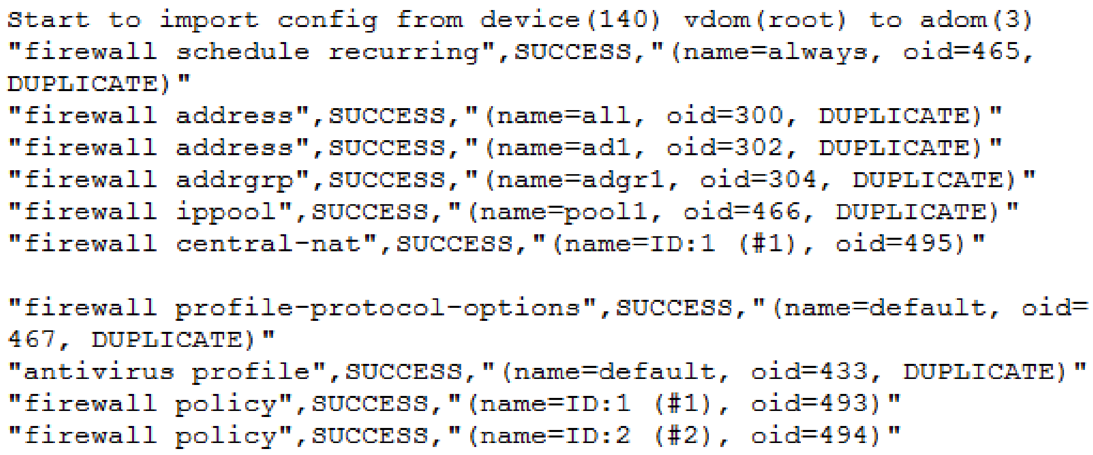


Figure 131: Summary example

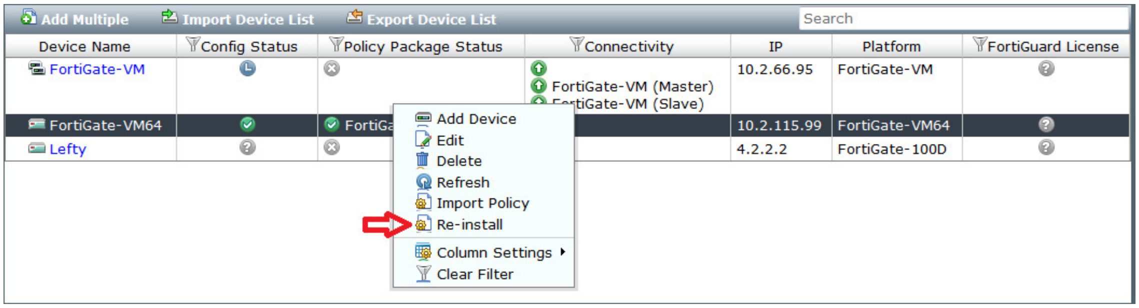


```
Start to import config from device(140) vdom(root) to adom(3)
"firewall schedule recurring",SUCCESS,"(name=always, oid=465,
DUPLICATE)"
"firewall address",SUCCESS,"(name=all, oid=300, DUPLICATE)"
"firewall address",SUCCESS,"(name=ad1, oid=302, DUPLICATE)"
"firewall addrgrp",SUCCESS,"(name=adgr1, oid=304, DUPLICATE)"
"firewall ippool",SUCCESS,"(name=pool1, oid=466, DUPLICATE)"
"firewall central-nat",SUCCESS,"(name=ID:1 (#1), oid=495)"

"firewall profile-protocol-options",SUCCESS,"(name=default, oid=
467, DUPLICATE)"
"antivirus profile",SUCCESS,"(name=default, oid=433, DUPLICATE)"
"firewall policy",SUCCESS,"(name=ID:1 (#1), oid=493)"
"firewall policy",SUCCESS,"(name=ID:2 (#2), oid=494)"
```

Using quick install

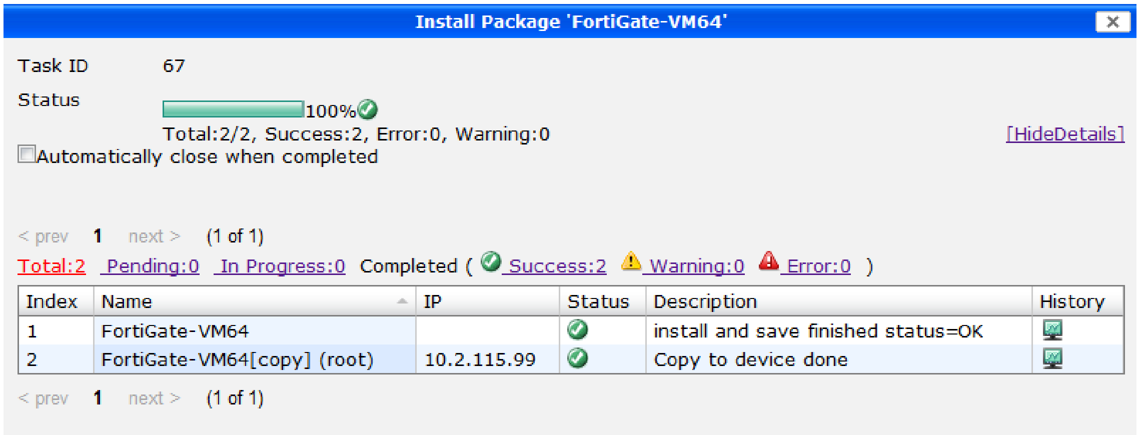
You can right-click on the Policy Config Status column icon to perform a quick install of a policy package without launching the *Install wizard*. The content menu is disabled when the policy package is already in sync. You can also right-click on the Config Status if the device is out of sync to install any device setting changes. This will only affect the settings for the selected device.

Figure 132: Right-click options



Device Name	Config Status	Policy Package Status	Connectivity	IP	Platform	FortiGuard License
FortiGate-VM	◷	⊗	↑ ↑ FortiGate-VM (Master) ↑ FortiGate-VM (Slave)	10.2.66.95	FortiGate-VM	?
FortiGate-VM64	✓	✓ FortiGa		10.2.115.99	FortiGate-VM64	?
Lefty	?	⊗		4.2.2.2	FortiGate-100D	?

Figure 133:reinstall a policy package



Task ID 67

Status 100% ✓

Total:2/2, Success:2, Error:0, Warning:0

□ Automatically close when completed

< prev 1 next > (1 of 1)

Total:2 Pending:0 In Progress:0 Completed (✓ Success:2 ⚠ Warning:0 ⚠ Error:0)

Index	Name	IP	Status	Description	History
1	FortiGate-VM64		✓	install and save finished status=OK	🖥
2	FortiGate-VM64[copy] (root)	10.2.115.99	✓	Copy to device done	🖥

< prev 1 next > (1 of 1)

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.

This section contains the following topics:

- Checking device configuration status
- Managing configuration revision history

Checking device configuration status

In the *Device Manager* tab, when you select a device, you can view that device's basic information under the *device dashboard*. You can also check if the current configuration file of the device stored in the FortiManager repository is in sync with the one running on the device.

If you make any configuration changes to a device directly, rather than using the FortiManager system, the configuration on the device and the configuration saved in the FortiManager repository will be out of sync. In this case, you can re synchronize with the device by retrieving the configuration from the device and saving it to the FortiManager repository.

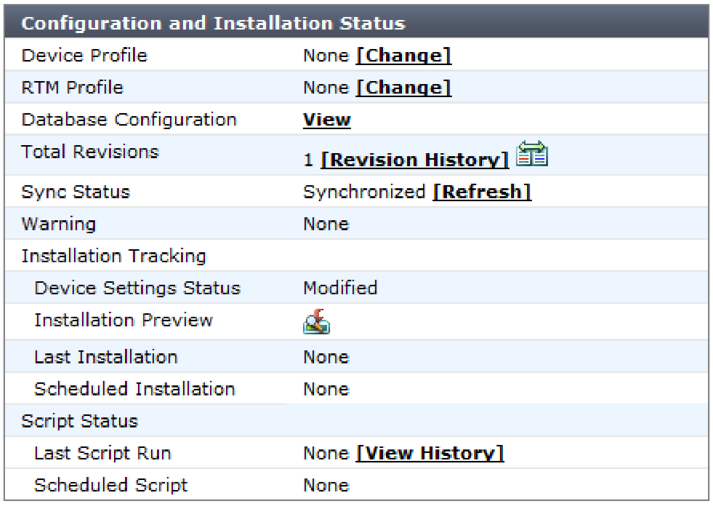
You can use the following procedures when checking device configuration status on a FortiGate, FortiCarrier, or FortiSwitch.

To check the status of a configuration installation on a FortiGate unit:

1. Go to the *Device Manager* tab, then select the ADOM and device group.
2. On the *All FortiGate* page, select the FortiGate unit that you want to check the configuration status of.

   The device dashboard of for that unit is shown in the lower content pane.
3. On the dashboard, locate the *Configuration and Installation Status* widget.
4. Verify the status in the *Installation Tracking* section.

Figure 134: Configuration and Installation Status widget



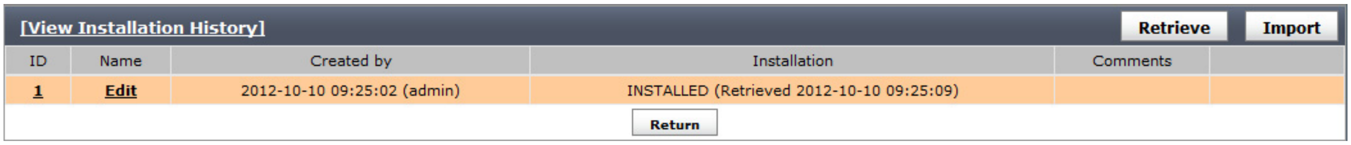
Configuration and Installation Status	
Device Profile	None [Change]
RTM Profile	None [Change]
Database Configuration	View
Total Revisions	1 [Revision History]
Sync Status	Synchronized [Refresh]
Warning	None
Installation Tracking	
Device Settings Status	Modified
Installation Preview	
Last Installation	None
Scheduled Installation	None
Script Status	
Last Script Run	None [View History]
Scheduled Script	None

Device Profile	Whether the device is associated with a device profile. Select *[Change]* to select a device profile to associate with the device.
RTM Profile	The RTM profile associated with the device. Select *[Change]* to select a different RTM profile to associate with the device.
Database Configuration	Select *View* to view the device configuration.
Total Revisions	Select *[Revision History]* to view the device revision history. Select the icon to the right to set the *Revision Diff*.
Sync Status	Displays the synchronization status with the FortiManager device. Select *[Refresh]* to force refresh the connection status. The device will attempt to re-establish a connection with the FortiManager.
Warning	Displays connection errors.
Installation Tracking	
Device Settings Status	Displays the device setting status. If no changes have been made, Unmodified will be displayed.
Installation Preview	Select the icon to view preview the installation.
Last Installation	The date of the last installation. If the device has not been installed, None will be displayed.
Scheduled Installation	The date of the scheduled installation. If the device has not been installed, None will be displayed.
Script Status	
Last Script Run	**Displays the date that the last script was run. Select [View History] to view the script execution history.**
Scheduled Script	**Displays the date of the scheduled script.**

Managing configuration revision history

On the *Device Manager* tab, select a device on the tree-menu. On the device dashboard *Configuration and Installation Status* widget, select *Revision History* in the *Total Revisions* row, to view the FortiManager repository.

Figure 135: Revision history tab



ID	Name	Created by	Installation	Comments	
1	Edit	2012-10-10 09:25:02 (admin)	INSTALLED (Retrieved 2012-10-10 09:25:09)		

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.

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 194.

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 193 and "To download a configuration file to a local computer:" on page 194.

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.

Comments Display the comment added to this configuration file when you edit the file name.

Diff icon Show only the changes or differences between two versions of a configuration file. See “Comparing different configuration files” on page 194 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. See “To revert to another configuration file:” on page 195.

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

To view the configuration settings on a FortiGate unit:

1. On the content pane with a device already selected, go to the *Configuration and Installation Status* widget*,* on the *Total Revisions* row, select *Revision History*.
2. Select the *ID* for the revision you want to view.

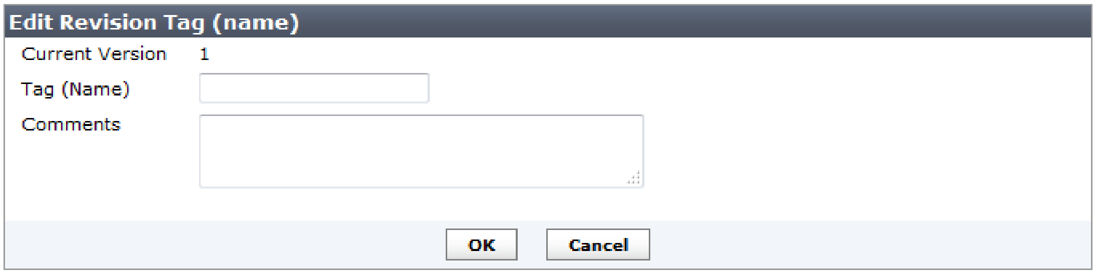
   You are automatically redirected to the View Configuration page.
3. Select *Return* when you finish viewing.

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 194.

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

1. On the content pane with a device already selected, go to the *Configuration and Installation Status* widget*,* on the *Total Revisions* row, select *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*.

Figure 136: Add a tag to a configuration version



Edit Revision Tag (name)

Current Version 1

Tag (Name)

Comments

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.

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. On the content pane with a device already selected, go to the *Configuration and Installation Status* widget*,* on the *Total Revisions* row, select *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. On the content pane with a device already selected, go to the *Configuration and Installation Status* widget*,* on the *Total Revisions* row, select *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* 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.

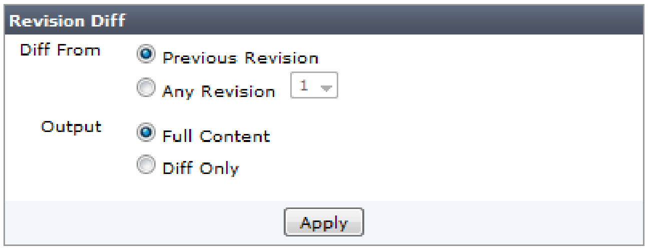
To compare different configuration files:

1. On the content pane with a device already selected, go to the *Configuration and Installation Status* widget*,* on the *Total Revisions* row, select *Revision History*.
2. On the *Total Revisions* row, select the *Revision Diff* icon, .
3. Select either the previous version or specify a different configuration version to compare in *Diff From*.
4. 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.
5. Select *Apply*.

   The configuration differences are displayed in colored highlights:

Figure 137: Revision *diff* dialog box



Revision Diff

Diff From ● Previous Revision
○ Any Revision 1

Output ● Full Content
○ Diff Only

Apply

To revert to another configuration file:

1. On the content pane with a device already selected, go to the *Configuration and Installation Status* widget*,* on the *Total Revisions* row, select *Revision History*.
2. Select the *Revert* icon for the revision you want to revert to.
3. Select *OK*.

Advanced Features

This chapter includes:

- Scripting
- Configuring web portals

Additional configuration options and short-cuts are available using the right-click menu. Right-click the mouse on different navigation panes on the Web-based Manager page to access these options.

Scripting

FortiManager scripts enable you to create, execute, and view the results of scripts executed on FortiGate devices, policy packages, the ADOM database, the global policy package, or the DB. Scripts can also be filtered based on different device information, such as OS type and platform.

At least one FortiGate device must be configured on the FortiManager system for you to be able to use scripts.

Any scripts that are run on the global database must use complete commands. For example, if the full command is `config system global`, do not use `conf sys glob`.

Scripts can be written in one of two formats:

- A sequence of FortiGate CLI commands, as you would type them at the command line. A comment line starts with the number sign (#). A comment line will not be executed.
- TCL scripting commands to provide more functionality to your scripts including global variables and decision structures.

When writing your scripts, it is generally easier to write them in a context-sensitive editor, and then cut and paste them into the script editor on your FortiManager system. This can help avoid syntax errors and can reduce the amount of troubleshooting required for your scripts.

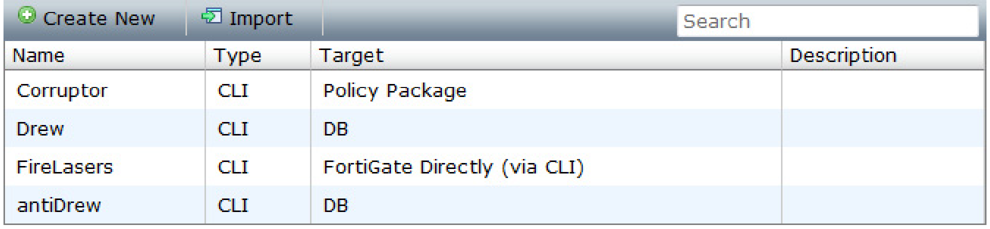
For information about scripting commands, see the *FortiGate CLI reference*.

Before using scripts, ensure the `console-output` function has been set to `standard` in the FortiGate CLI. Otherwise, scripts and other output longer than a screen in length will not execute or display correctly.

Configuring scripts

To configure, import, export, or run scripts, go to the *Device Manager* tab, expand an ADOM view in the tree menu, and then select *Script* > *Script*. The script list for the selected ADOM will be displayed.

Figure 138: Script list



Name	Type	Target	Description
Corruptor	CLI	Policy Package	
Drew	CLI	DB	
FireLasers	CLI	FortiGate Directly (via CLI)	
antiDrew	CLI	DB	

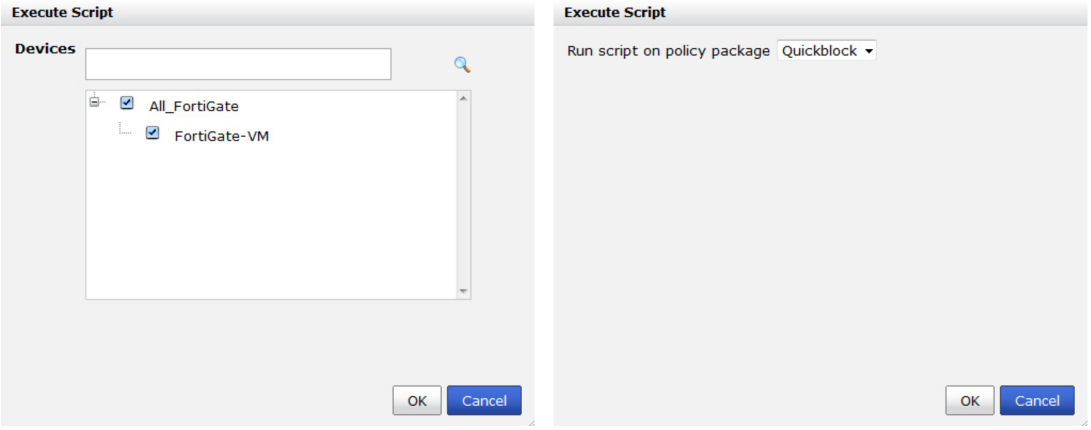
Run a script

To run a script:

1. Browse to the ADOM script list for the ADOM that contains the script you would like to run.
2. Select the script, then right-click and select *Run* from the pop-up menu.

   The *Execute Script* dialog box will open. This dialog box will vary depending on the script target. You will either be able to select a device or devices (left image below), or a policy package (right image). See "Override Script Target" on page 199 for more information.

   Figure 139: Execute script dialog boxes

   Execute Script

   Devices

   ☑ All_FortiGate
   ☑ FortiGate-VM

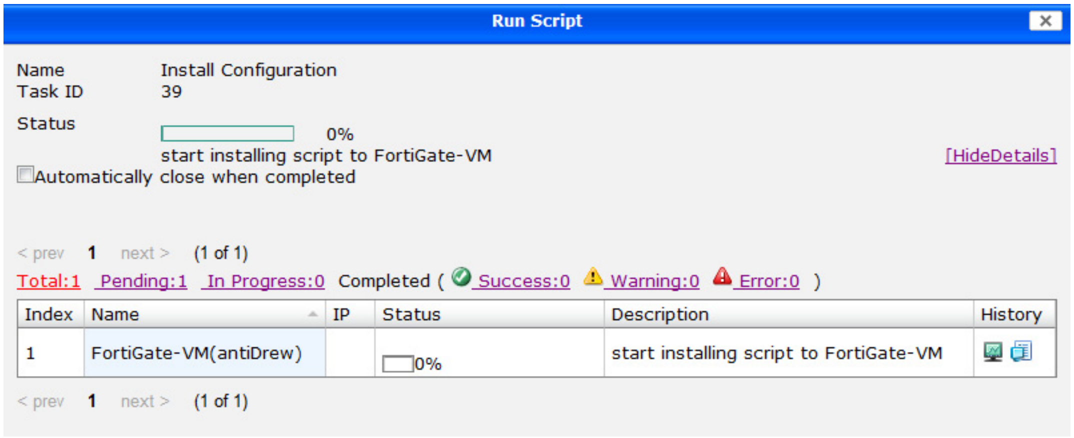
   Execute Script

   Run script on policy package Quickblock

3. Select *OK* to run the script.

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

Figure 140: Run script dialog box



Run Script

Name Install Configuration
Task ID 39
Status 0%
start installing script to FortiGate-VM

[HideDetails]

□ Automatically close when completed

< prev 1 next > (1 of 1)

Total:1 Pending:1 In Progress:0 Completed (Success:0 Warning:0 Error:0)

Index	Name	IP	Status	Description	History
1	FortiGate-VM(antiDrew)		0%	start installing script to FortiGate-VM	

< prev 1 next > (1 of 1)

4. Selecting the *Details* option will expand the dialog box to show the details table, with details of the success or failure of the script.

   Under the *History* column in the details table, you can select the *History* icon to open the script history for that device, and the *View Script Execution History* icon to view the script execution history for that device.

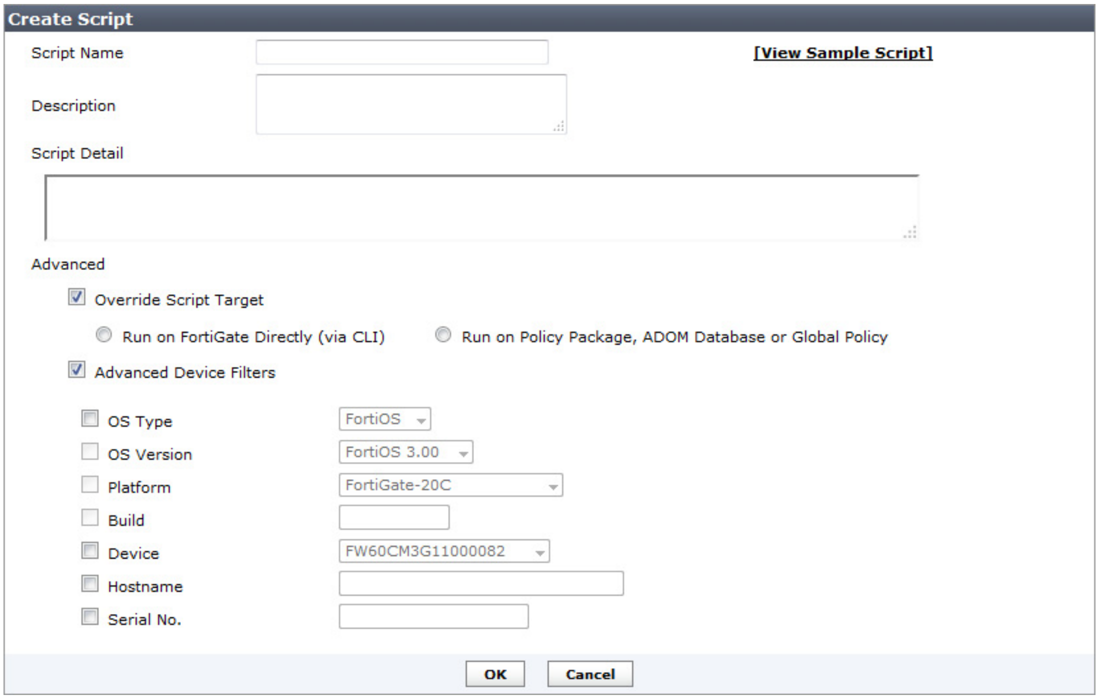
5. Close the *Run Script* dialog box when finished.

Add a script

To add a script to an ADOM:

1. Browse to the ADOM script list for the ADOM in which you will be creating the script.
2. Select *Create New*, or right-click anywhere in the script list and select *New* from the pop-up menu, to open the *Create Script* dialog box.

Figure 141: Create a new script



Create Script

Script Name [View Sample Script]

Description

Script Detail

Advanced

☑ Override Script Target

○ Run on FortiGate Directly (via CLI) ○ Run on Policy Package, ADOM Database or Global Policy

☑ Advanced Device Filters

□ OS Type	FortiOS
□ OS Version	FortiOS 3.00
□ Platform	FortiGate-20C
□ Build	
□ Device	FW60CM3G11000082
□ Hostname	
□ Serial No.	

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

Script Name Enter a name for the script.

View Sample Script Select this link to view sample scripts.

Description Optionally, enter a description of your script.

Script Detail Enter the script itself, either manually using a keyboard, or by copying and pasting from another editor.

Override Script Target Select to change the script target. This settings will affect the options presented when you go to run a script. The options include:

- *Run on FortiGate Directly (via CLI)*
- *Run on Policy Package, ADOM Database or Global Policy*
- *Run on DB* (default).

Advanced Device Filter Select to adjust the advanced filters for the script. The options include:

- *OS Type* (select from the drop-down list)
- *OS Version* (select from the drop-down list)
- *Platform* (select from the drop-down list)
- *Build*
- *Device* (select from the drop-down list)
- *Hostname*
- *Serial No.*

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

Edit a script

All of the same options are available when editing a script as when creating a new script, except the name of the script cannot be changed.

To edit a script, from the script list of the selected ADOM, either double click on the name of the script, or right-click on the script name and select *Edit* from the pop-up menu. The *Edit Script* dialog box will open, allowing you to edit the script and its settings.

Clone a script

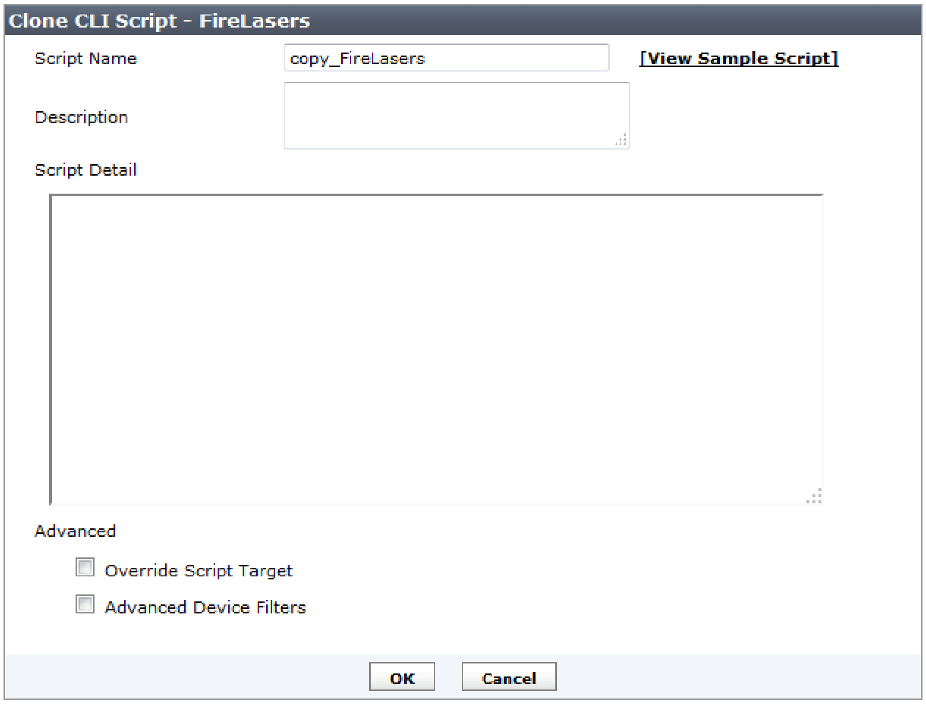
Cloning a script is useful when multiple scripts that are very similar.

To clone a script:

1. Browse to the ADOM script list for the ADOM with the script you would like to clone.
2. Select the script that you will be cloning, then right-click and select *Clone* from the pop-up menu.

   The *Clone Script* dialog box will open, showing the exact same information as the original, except *copy_* is appended to the script name.

Figure 142: Clone script dialog box



Clone CLI Script - FireLasers

Script Name: copy_FireLasers

3. Edit the script and its settings as needed and select *OK* to create the clone.

Delete a script

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

Export a script

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

To export a script:

1. Browse to the ADOM script list for the ADOM with the script you would like to export.
2. Select the script that you will be exporting, then right-click and select *Export* from the pop-up menu.
3. If prompted by your web browser, select a location to where save the file, or open the file without saving, then select *OK*.

Import a script

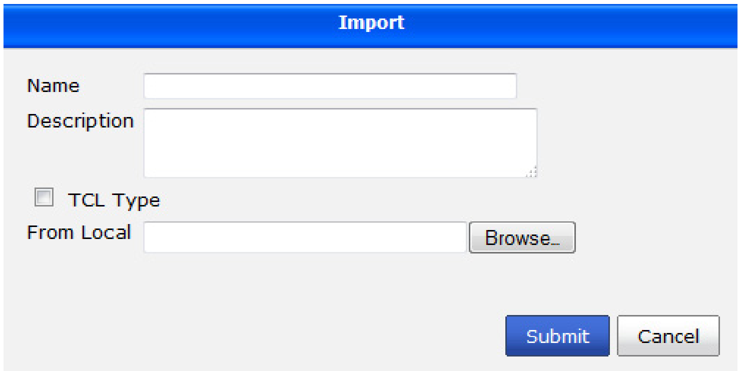
Scripts can be imported as text files from your local computer.

To import a script:

1. Browse to the ADOM script list for the ADOM you will be importing the script to.
2. Select *Import* from the toolbar.

   The Import dialog box opens.

Figure 143: Import script dialog box



3. Enter a name and description for the script you are importing.
4. Select *TCL Type* if the script you are importing is a TCL script.
5. Select *Browse* and locate the file to be imported on your local computer.
6. Select *Submit* to import the script.

   If the script cannot be read, due to an incorrect file type or other issue, an error message will be displayed and the import process will be cancelled.

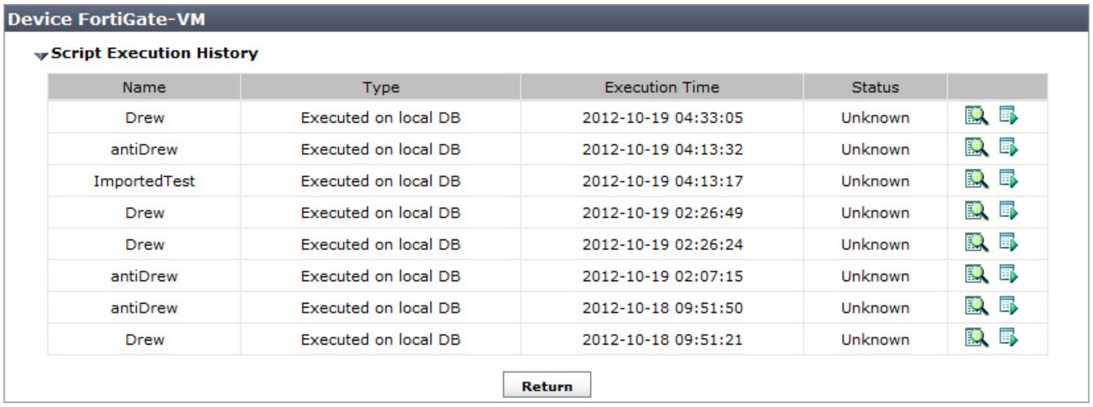
Script history

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

To view the script execution history:

1. In *Device Manager*, locate the device whose script history you want to view.
2. In the lower content pane, select *Dashboard*, and find the *Configuration and Installation Status widget*.
3. Select *Configure* in the *Script Status* field of the widget to open the *Script Execution History table*.

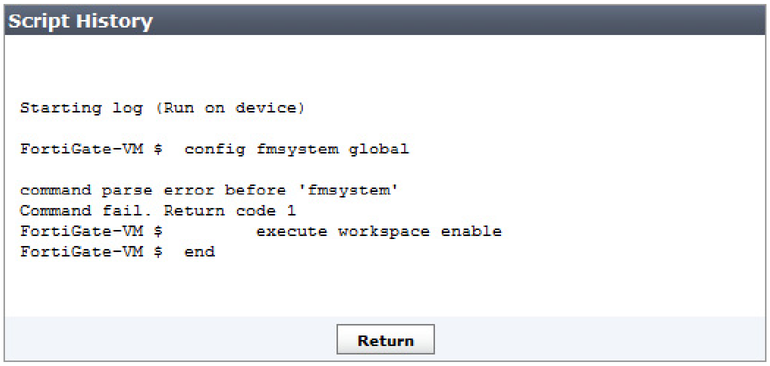
Figure 144: Script execution history table



Name	Type	Execution Time	Status	
Drew	Executed on local DB	2012-10-19 04:33:05	Unknown	🔍 ➡
antiDrew	Executed on local DB	2012-10-19 04:13:32	Unknown	🔍 ➡
ImportedTest	Executed on local DB	2012-10-19 04:13:17	Unknown	🔍 ➡
Drew	Executed on local DB	2012-10-19 02:26:49	Unknown	🔍 ➡
Drew	Executed on local DB	2012-10-19 02:26:24	Unknown	🔍 ➡
antiDrew	Executed on local DB	2012-10-19 02:07:15	Unknown	🔍 ➡
antiDrew	Executed on local DB	2012-10-18 09:51:50	Unknown	🔍 ➡
Drew	Executed on local DB	2012-10-18 09:51:21	Unknown	🔍 ➡

4. To view the script history for a specific script, select the *Browse* icon in the far right column of the table to open the *Script History* dialog box.

Figure 145: Script history dialog box.



```
Starting log (Run on device)

FortiGate-VM $  config fmsystem global

command parse error before 'fmsystem'
Command fail. Return code 1
FortiGate-VM $         execute workspace enable
FortiGate-VM $  end
```

5. To re-run a script, select the Run script now icon in the far right column of the table.

   The script is re-run. See "Run a script" on page 197 for more information.
6. Select *Return* to return to the device dashboard.

Configuring web portals

The web portal enables MSSP customers to manage their own SSL-VPN user list, web filtering, URL filters, and categories. If configured, customers can also view the firewall policies on their FortiGate devices or VDOM.

You create a portal profile and include its content and appearance. You can then 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 to a specific 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 does not have access to the FortiManager Web-based Manager.

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. Once set up, portal users, or administrators, can be added to the portal.

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 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.

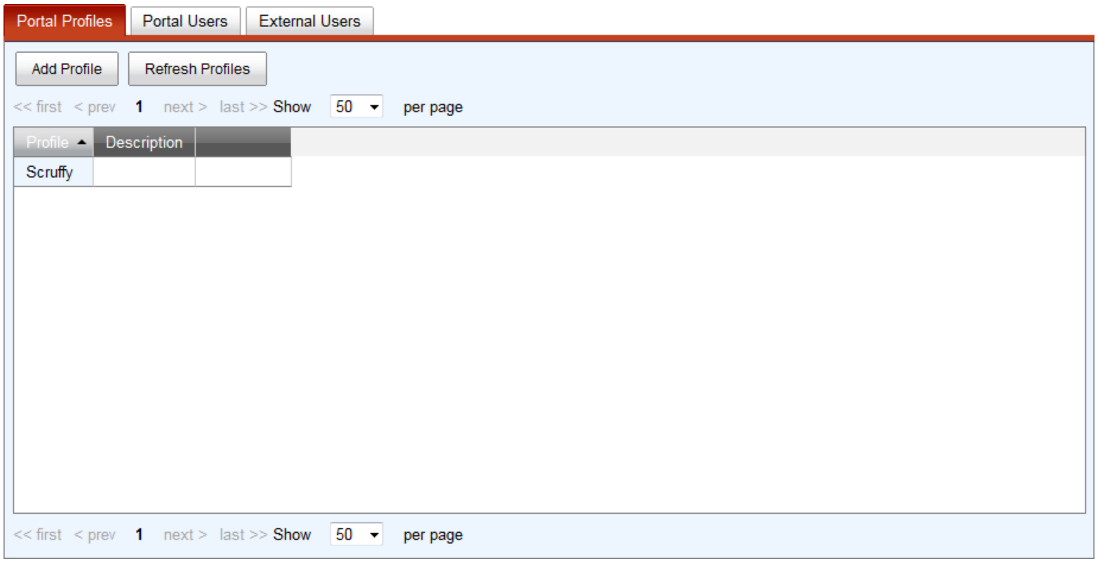
Creating a web portal

Before creating a web portal, ensure you have an ADOM 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. In the device manager tab, select the ADOM in which the web portal will be created.
2. Select *Web Portal*.

Figure 146: Web portal window

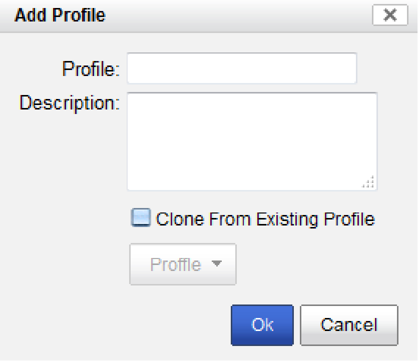

Portal Profiles
Portal Users
External Users
Add Profile
Refresh Profiles
<< first < prev 1 next > last >> Show 50 per page
<< first < prev 1 next > last >> Show 50 per page

Profile ▲	Description
Scruffy	

Show Web Portal must be selected in the Admin Settings. See "Administrator settings" on page 90 for more information.

3. Select *Add Profile* to open the *Add Profile* dialog box.

Figure 147: Add profile dialog box



4. In the *Profile* field, enter a name for the profile, and optionally, enter a description in the *Description* field. The profile name can be a maximum of 35 characters and cannot contain spaces.

5. 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.
6. Select *OK*.

Configuring the web portal profile

With the web portal profile added, you can configure the portal with the available widgets.

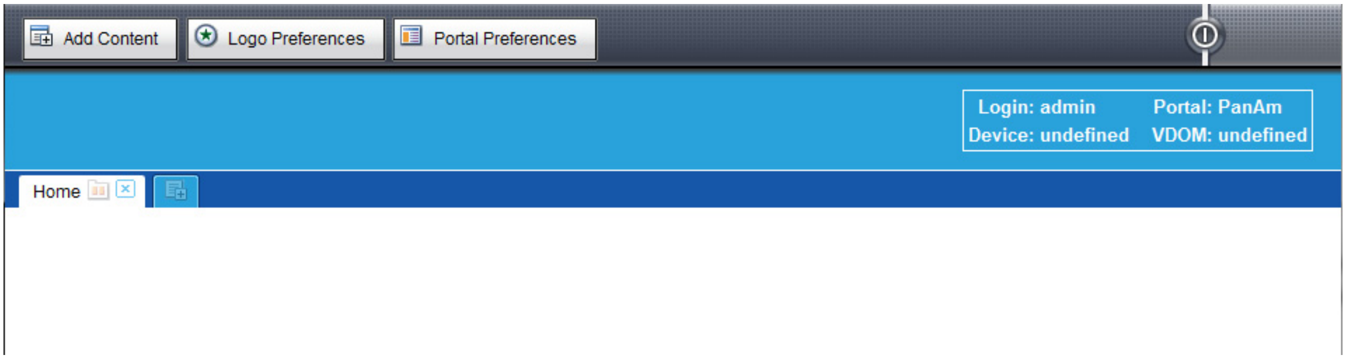
To configure the web portal profile:

1. On the web portal screen, select a profile from the list.
2. Either select the *Configure Profile* icon for the profile, or right click on the profile and select *Configure Profile* from the pop-up menu.

   The *Configure Profile* dialog box opens.
3. 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.

Figure 148: Blank web portal window



Login: admin
Portal: PanAm
Device: undefined
VDOM: undefined

Modifying the content and layout

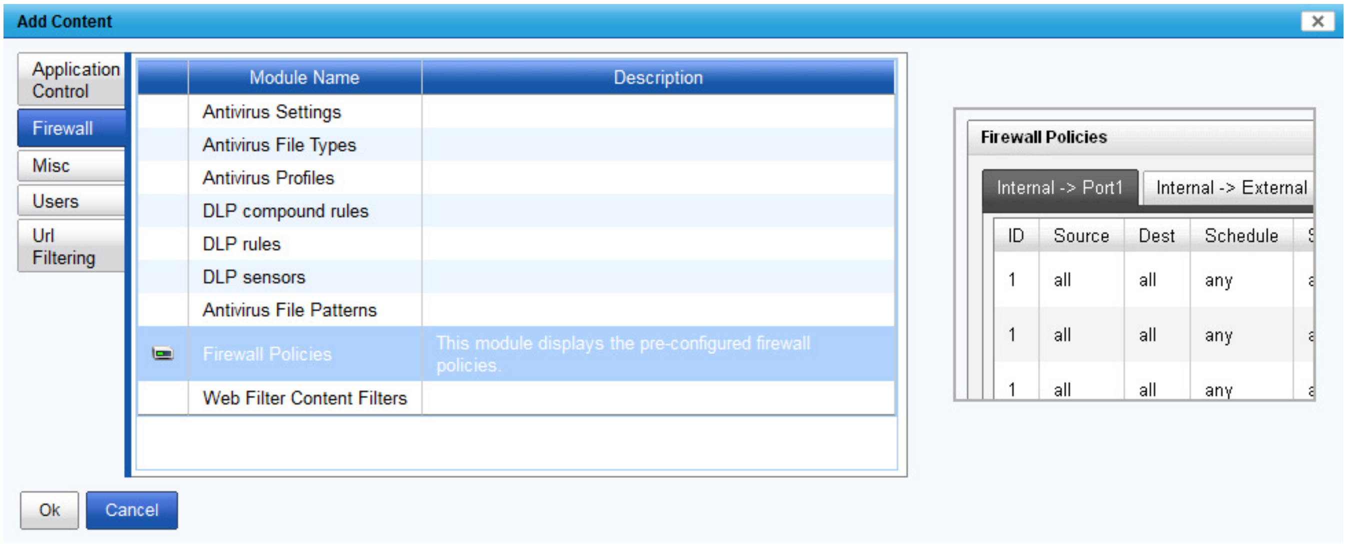
The web portal design window enables you to add content for the user’s internet and firewall connection and arrange the layout of the information.

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 149: Adding web portal content



Add Content

	Module Name	Description
	Antivirus Settings	
	Antivirus File Types	
	Antivirus Profiles	
	DLP compound rules	
	DLP rules	
	DLP sensors	
	Antivirus File Patterns	
	Firewall Policies	This module displays the pre-configured firewall policies.
	Web Filter Content Filters	

Firewall Policies

ID	Source	Dest	Schedule	S
1	all	all	any	a
1	all	all	any	a
1	all	all	any	a

A number of content options are available. Select a tab on the left to view the available widgets. To add a particular widget, either double-click to add the content, or select a widget and select *OK*. Holding the CTRL or Shift keys on your keyboard enables you to select multiple widgets at the same time.

Once you have selected the widgets, you can move them on the page within the chosen column view.

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 that line to the 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 to the widget.

You can resize the widgets vertical size by clicking and dragging the bottom of the widget

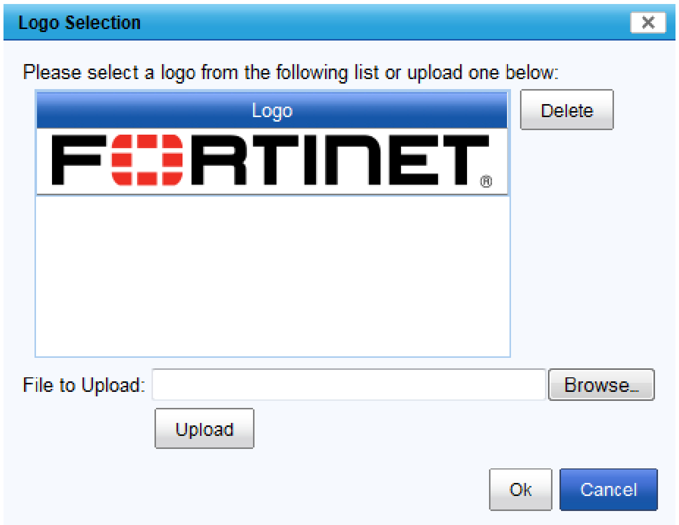
Adding a logo

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.

To add a logo to the web portal display:

1. Select *Logo Preferences*.

Figure 150: Logo preferences



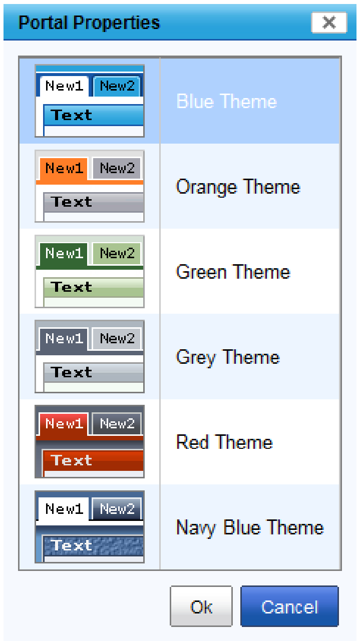
Please select a logo from the following list or upload one below:

2. Select *Browse* and locate the desired logo on your hard disk or network volume.
3. Select *Upload*.
4. Select the uploaded logo in the logo list, and then 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*.

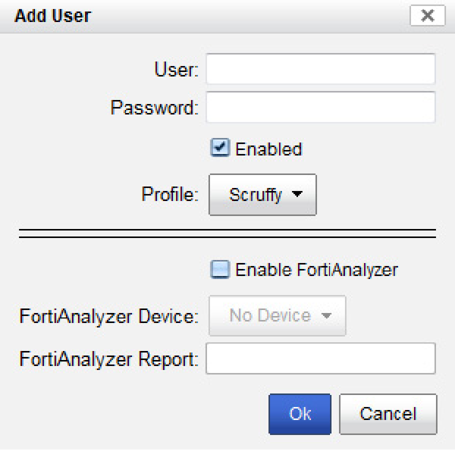
Figure 151: Portal properties window



Creating a portal user account

To create a portal user account, in the Web Portal screen of the selected ADOM, select the *Portal Users* tab, and then select *Add User*. The *Add User* dialog box will open.

Figure 152: Add user dialog box



User:

Password:

☑ Enabled

Profile: Scruffy

☐ Enable FortiAnalyzer

FortiAnalyzer Device: No Device

FortiAnalyzer Report:

Enter the below information and then select OK to create the new portal user.

User	Enter the name of the user who will log into the portal. The user name must be 35 or less characters.
Password	Enter the password for the user. The password must be 20 or less characters.
Enabled	Select to enable the user profile.
Profile	Select the web portal profile that this user will log into from the drop-down list.
Enable FortiAnalyzer	Select to enable a FortiAnalyzer device to use the profile.
FortiAnalyzer Device	Select a FortiAnalyzer device from the drop-down list.
FortiAnalyzer Report	Enter the name of the FortiAnalyzer report.

External users

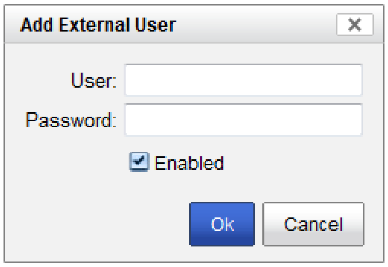
Use the *External Users* tab to add external users. This enables users to have remote access to the managing FortiManager unit from the portal FortiManager unit.

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. In the *Web Portal* screen, select the *External Users* tab.
2. Select *Add External User*.

Figure 153: Add external user window



3. Enter the required information and select *OK*.

User Enter a name for the external user.

Password Enter a password for the external user.

Enabled Select to enable the external user.

Using the web portal

The purpose of the web portal is to enable customers, or their administrators to monitor and maintain their firewall settings.

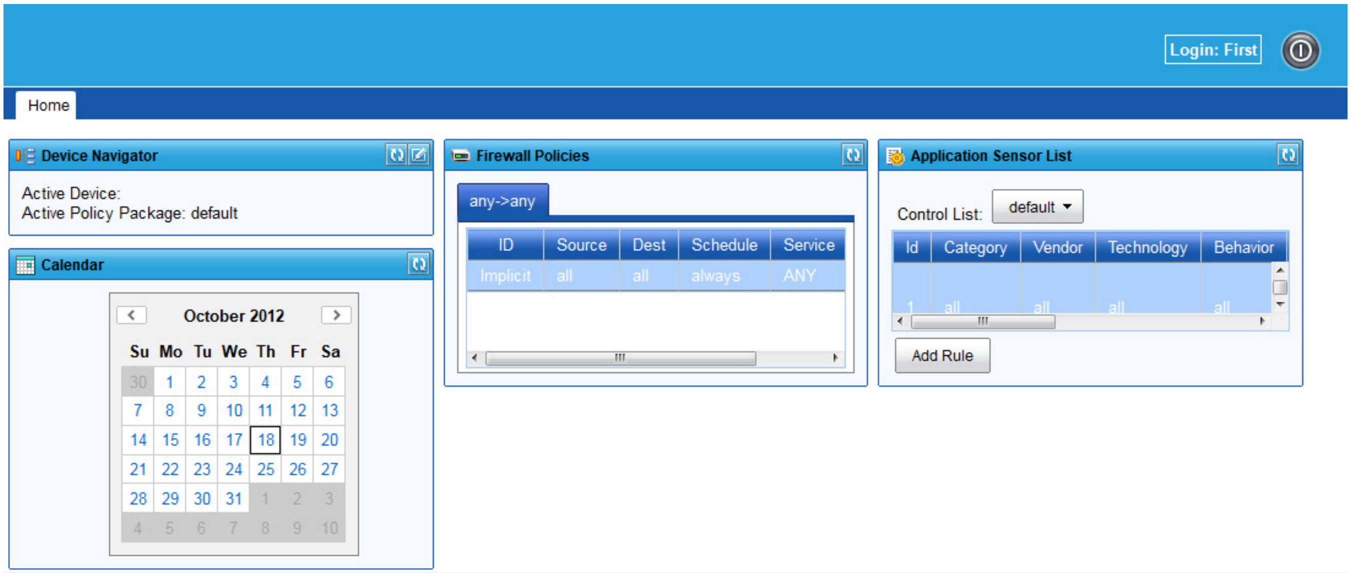
Before the users can use the web portal you need to supply them with the following information:

- the URL or IP address of the FortiManager system
- their user name
- their 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.

Figure 154: Web portal



Active Device:
Active Policy Package: default

October 2012

Su	Mo	Tu	We	Th	Fr	Sa
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

ID	Source	Dest	Schedule	Service
Implicit	all	all	always	ANY

Control List: default

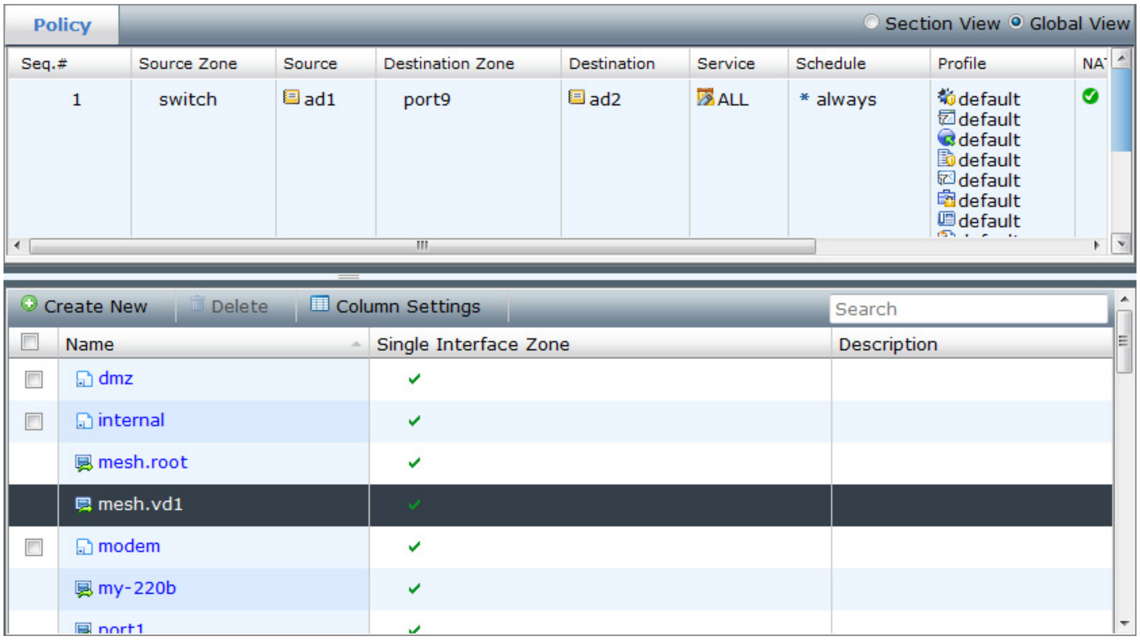
Id	Category	Vendor	Technology	Behavior
1	all	all	all	all

Policy & Objects

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

If the administrator account you logged on with does not have the appropriate 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 “Profile” on page 83.

Figure 155: Policy & Objects



Seq.#	Source Zone	Source	Destination Zone	Destination	Service	Schedule	Profile	NA
1	switch	ad1	port9	ad2	ALL	always	default default default default default default default	✓

□	Name	Single Interface Zone	Description
□	dmz	✓	
□	internal	✓	
	mesh.root	✓	
	mesh.vd1	✓	
□	modem	✓	
	my-220b	✓	
	port1	✓	

If workspace is enabled, an ADOM must be locked before any changes can made to policy packages or objects. See “Concurrent ADOM access” on page 44 for information on enabling or disabling workspace.

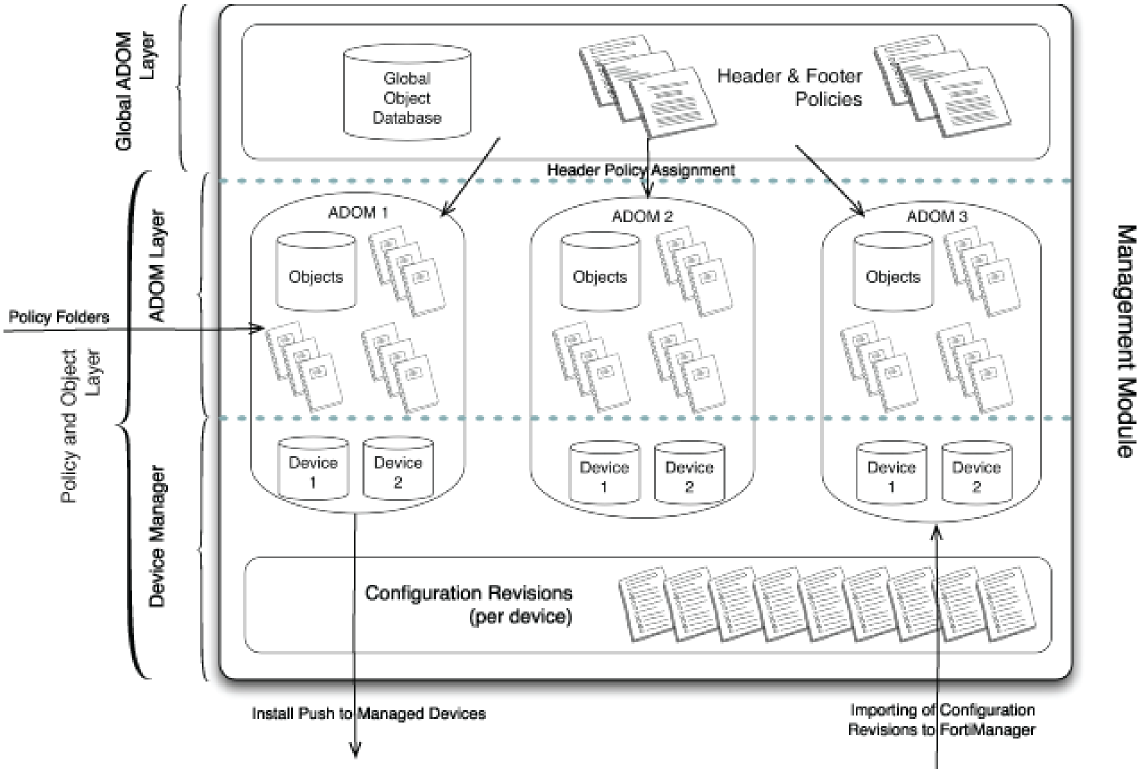
About policies

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

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

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

Figure 156: Management model



Policy theory

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

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

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

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

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

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

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

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

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

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

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

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

Global policy packages

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

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

Global policy packages must be explicitly assigned to specific ADOMs to be used. When configuring global policies, a block of space in the policy table is reserved for *Local Domain Policies*. All of the policies in an ADOM's policy table is inserted into this block when the global policy is assigned to an ADOM.

Display options for policies and objects can be configured in *System Settings* > *Admin* > *Admin Settings.*

Global policies and objects are not supported on all FortiManager platforms. Please review the products' datasheets to determine support.

A global policy license is not required to use global policy packages.

Policy workflow

An administrator will typically carry out 2 main functions with their devices through FortiManager: provisioning new devices or VDOMs on the network and managing the day-to-day operations of managed devices and VDOMs.

Provisioning new devices

There are multiple steps to provision a new device or VDOM to be managed by the FortiManager unit:

1. In the *Device Manager*, create a new VDOM or add a new device.
2. Configure any Dynamic Objects you wish to assign to the new VDOM or device.
3. Determine how a policy will be defined for the new device: does the new device or VDOM have a new policy package unique to itself, or will use a package that is implemented elsewhere?
4. Run the *Install Wizard* to install any objects and policies for the new device, or create a new policy package.
5. If the new device uses an existing policy package, modify the Installation Targets of that package to include the new device and click *Install*.

Day-to-day management of devices

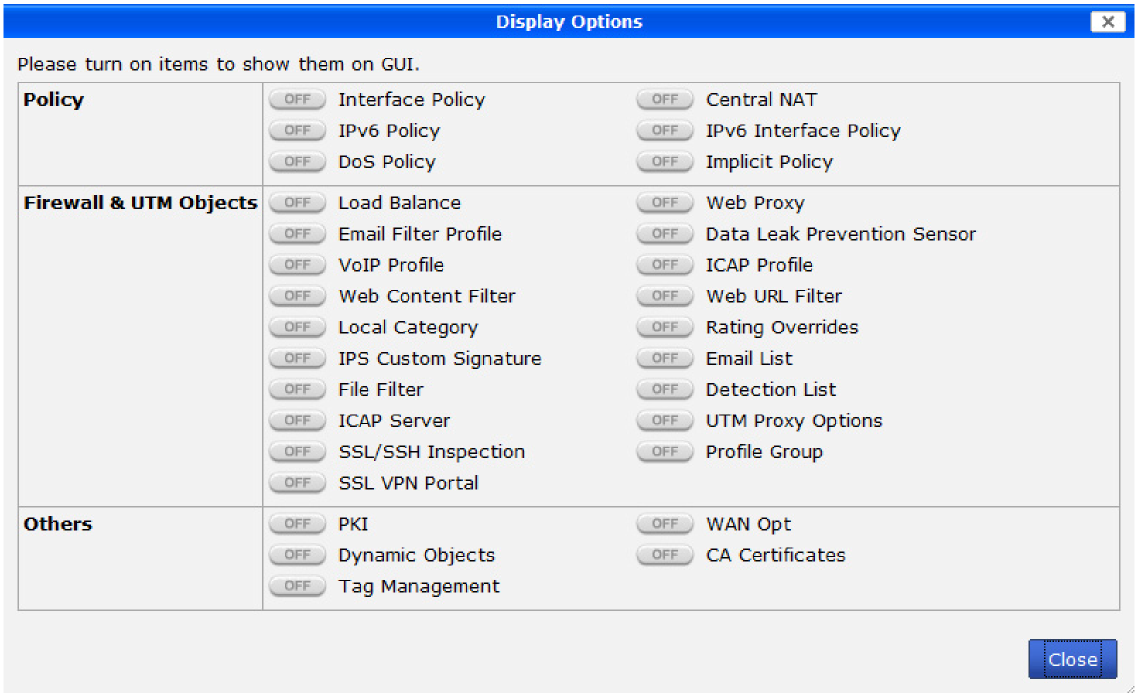
An administrator will often have to modify various objects for the devices they are responsible for managing. A typical set of tasks to manage an already provisioned device will include:

1. Adding, deleting, or editing various objects, such as firewall information, UTM profiles, User access rights, antivirus signatures, etc.
2. Adding, deleting, or editing all of the policy packages or individual policies within a policy package. This can include changing the order of operation, adding new policies, or modifying information or access privileges in the policy package.
3. Installing updates to devices.

Display Options

The objects that are displayed on the Policy & Objects page can be customized by selecting the *Edit* button in the toolbar. Customizations are per ADOM.

Figure 157: Display options



Please turn on items to show them on GUI.

Policy	OFF Interface Policy	OFF Central NAT
	OFF IPv6 Policy	OFF IPv6 Interface Policy
	OFF DoS Policy	OFF Implicit Policy
Firewall & UTM Objects	OFF Load Balance	OFF Web Proxy
	OFF Email Filter Profile	OFF Data Leak Prevention Sensor
	OFF VoIP Profile	OFF ICAP Profile
	OFF Web Content Filter	OFF Web URL Filter
	OFF Local Category	OFF Rating Overrides
	OFF IPS Custom Signature	OFF Email List
	OFF File Filter	OFF Detection List
	OFF ICAP Server	OFF UTM Proxy Options
	OFF SSL/SSH Inspection	OFF Profile Group
	OFF SSL VPN Portal	
Others	OFF PKI	OFF WAN Opt
	OFF Dynamic Objects	OFF CA Certificates
	OFF Tag Management	

Turn the various options on or off (visible or hidden) by selecting the on/off button next to their name. Once turned on, the corresponding options settings will be configurable from the appropriate location in the Polic & Objects tab.

Managing policy packages

Policy packages can be created and edited and then assigned to specific devices in the ADOM. Folders can be created for the policy packages to aid in the organization and management of the packages.

Not all policy and object options are enabled by default. To configure the enabled options, go to *System Settings > Admin > Admin Settings* and select your required options. See "Administrator settings" on page 90 for more information.

Lock an ADOM

If workspace is enabled, you must lock an ADOM prior to performing any management tasks on it.

To lock an ADOM:

1. Select the specific ADOM in which you are creating the policy folder from the drop-down list in the toolbar, or select *Global*.
2. Select the lock icon to lock the selected ADOM.

   The ADOM will now be locked, allowing you to make changes to it, and preventing other administrators from making any changes.

Create a new policy package or folder

To create a new policy folder:

1. Select the specific ADOM in which you are creating the policy folder from the drop-down list in the toolbar, or select *Global* to create a folder for global policy packages.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Folder* heading in the pop-up menu, select *Create New*.
4. Enter a name for the new policy folder in the dialog box and then select *OK*.

To create a new global policy package:

1. Select *Global* in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Package* heading in the pop-up menu, select *Create New*.

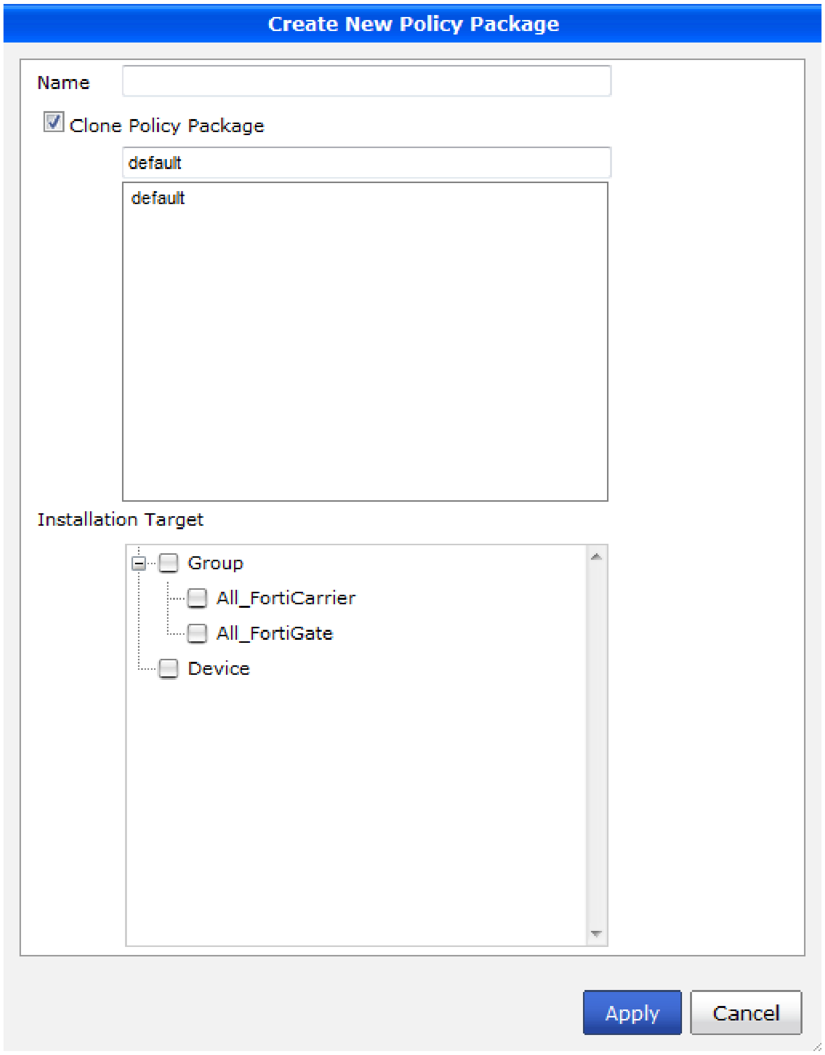
   The *Add Policy Package* dialog box opens.
4. Enter a name for the new global policy package in the dialog box.
5. If you are cloning a previous policy package, select *Clone Policy Package* and enter the name of the policy package you would like to clone in the resulting text field.
6. Select *OK* to add the policy package.

To create a new policy package:

1. Select the specific ADOM in which you are creating the policy package from the drop-down list in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Package* heading in the pop-up menu, select *Create New*.

   The *Create New Policy Package* dialog box opens.

Figure 158: Create new policy package



Create New Policy Package

Name

☑ Clone Policy Package

default

default

Installation Target

- □ Group
  - □ All_FortiCarrier
  - □ All_FortiGate
- □ Device

4. Enter a name for the new policy package in the dialog box.
5. If you are cloning a previous policy package, select *Clone Policy Package* and select the policy package you would like to clone from the list.
6. Select the targets to which you would like to install the new policy package.
7. Select *OK* to add the policy package.

Remove a policy package or folder

To remove a policy package or folder, right-click on the package or folder name in the policy package pane and select *Delete* from the pop-up menu.

Rename a policy package or folder

To rename a global policy package or policy package folder, right-click on the package or folder name in the policy package pane and select *rename* from the pop-up menu. Enter the new name for the global policy package or policy package folder in the pop-up dialog box and select *OK*.

To rename a local policy package, right-click on the policy package and select *Edit*. Enter the new name (or edit the current name) in the *Name* field of the *Edit Policy Package* dialog box and select *Apply*.

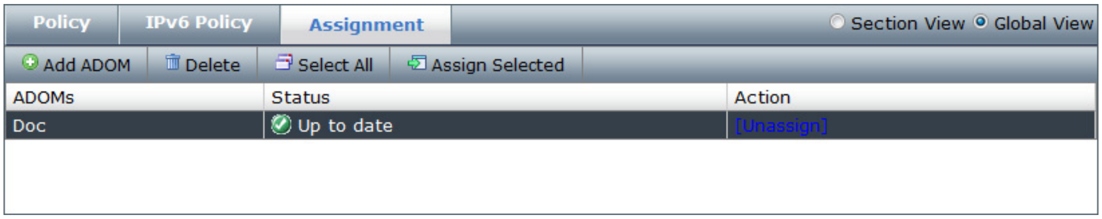
Assign a global policy package

Global policy packages can be assigned, or installed, to specific ADOMs.

To assign a global policy package:

1. Select *Global* in the toolbar and select a policy package in the *Policy Package* tree.
2. Select *Assignment* in the content pane tab bar to view the ADOM assignment list.

Figure 159:ADOM assignment list

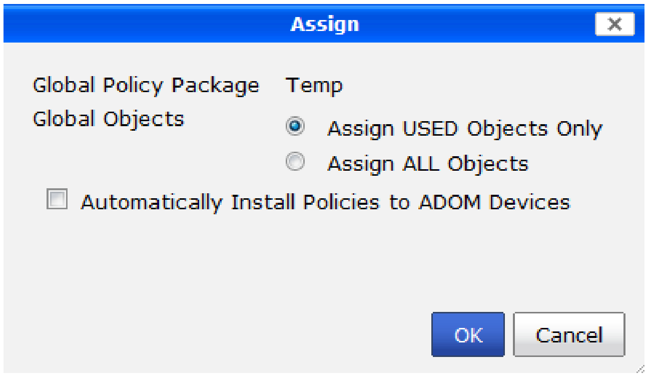


ADOMs	Status	Action
Doc	✓ Up to date	[Unassign]

3. If required, select *Add ADOM* from the content toolbar to add an ADOM to the list.
4. Select the ADOM you would like to assign from the list, or select *Select All* from the toolbar to select all of the ADOMs in the list.
5. Select *Assign Selected* from the toolbar.

   The *Assign* dialog box opens.

Figure 160: Assign dialog box



Global Policy Package Temp

Global Objects ● Assign USED Objects Only
○ Assign ALL Objects

□ Automatically Install Policies to ADOM Devices

6. Select whether you want to assign only used objects or all objects, and if policies will be automatically installed to ADOM devices.
7. Select *OK* to assign the policy package to the selected ADOM or ADOMs.

Install a policy package

To install a policy package to a target device:

1. Select the specific ADOM that contains the policy package you are installing from the drop-down list in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Package* heading in the pop-up menu, select *Install*.

   The install wizard opens.
4. Follow the steps in the install wizard to install the policy package.

   For more information, see "Install wizard" on page 176.

Export a policy package

To export a policy package:

1. Select the specific ADOM that contains the policy package you are exporting from the drop-down list in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Package* heading in the pop-up menu, select *Export*.

   If prompted by your web browser, select a location to where save the file, or open the file without saving.

   Policy packages are exported as CSV files.

Edit the installation targets for a policy package

To edit a policy package's installation targets:

1. Select the specific ADOM that contains the policy package you are exporting from the drop-down list in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Package* heading in the pop-up menu, select *Installation targets*.

   The *Installation Target* dialog box opens.
4. Adjust the installation targets as needed, then select *Apply*.

Perform a policy consistency check

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

The check will verify:

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

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

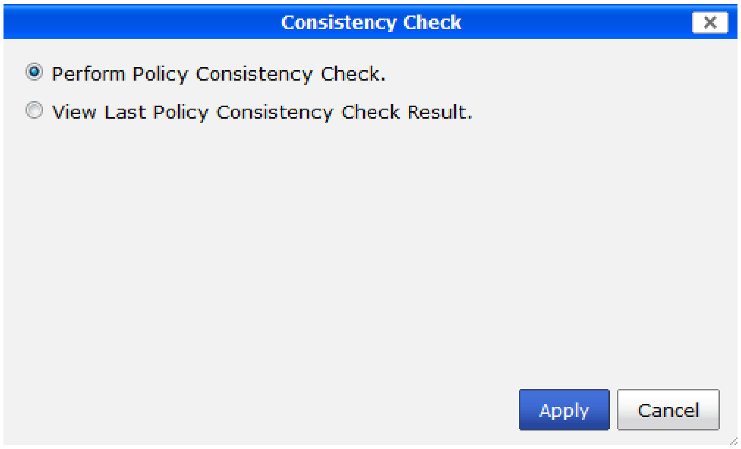
- The source and destination interface policy objects,
- The source and destination address policy objects,
- The service and schedule policy objects.

To perform a policy check:

1. Select the specific ADOM on which you would like to perform a consistency check from the drop-down list in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Package* heading in the pop-up menu, select *Policy Check*.

   The *Consistency Check* dialog box opens.

   Figure 161: Consistency Check dialog box



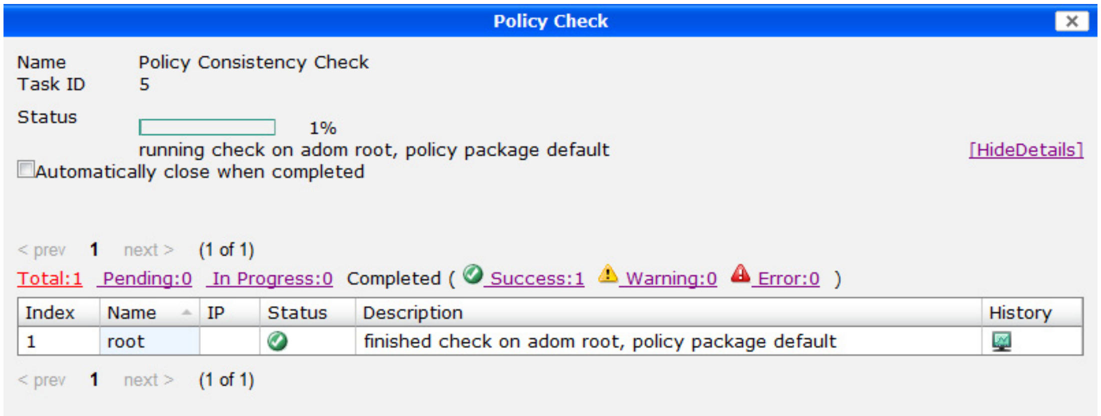
● Perform Policy Consistency Check.

○ View Last Policy Consistency Check Result.

4. To perform a new consistency check, select *Perform Policy consistency Check*, then select *Apply*.

   A policy consistency check is performed.
5. Select *Details* to view the details of the check will it is being performed. Select *Automatically close when complete* to close the dialog box automatically when the check completes.

   Figure 162: Policy Check dialog box



Name Policy Consistency Check
Task ID 5
Status 1%
running check on adom root, policy package default

□Automatically close when completed

Total:1 Pending:0 In Progress:0 Completed (Success:1 Warning:0 Error:0)

Index	Name	IP	Status	Description	History
1	root		✓	finished check on adom root, policy package default	

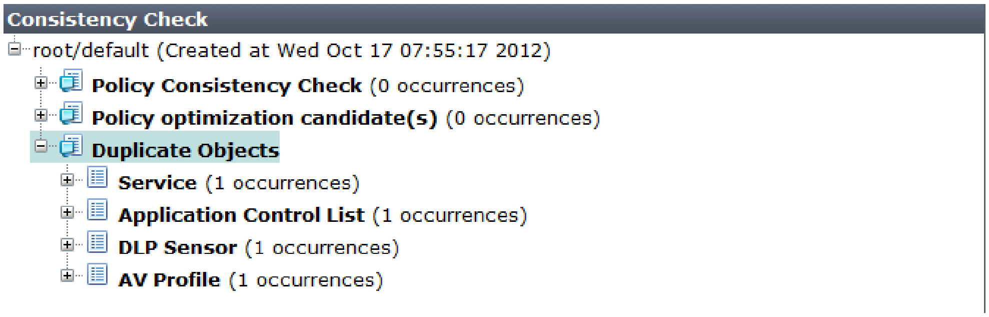
To view the results of the last policy consistency check:

1. Select the specific ADOM on which you would like to perform a consistency check from the drop-down list in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Package* heading in the pop-up menu, select *Policy Check*.

   The *Consistency Check* dialog box opens.
4. To view the results of the most recent consistency check, select *View Last Policy Consistency Check Results*, then select *Apply*.

   The Consistency Check window opens, showing the results of the last policy consistency check.

Figure 163: Consistency check results window



Consistency Check

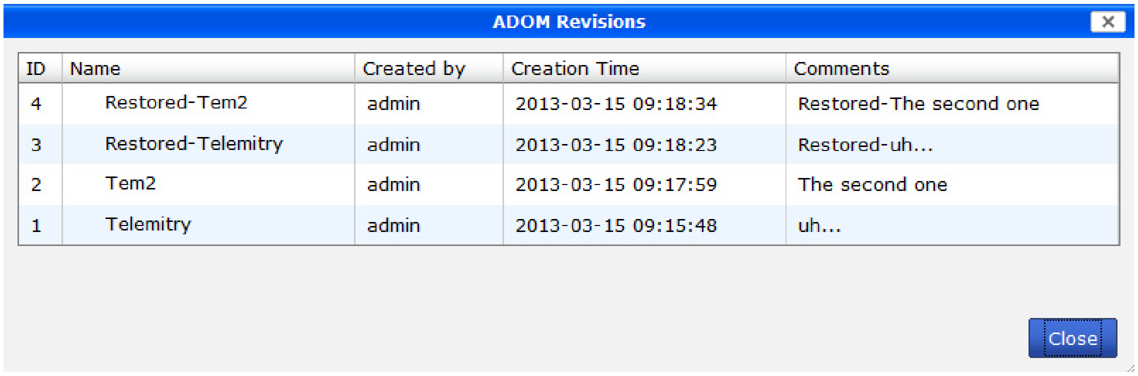
- root/default (Created at Wed Oct 17 07:55:17 2012)
  - **Policy Consistency Check** (0 occurrences)
  - **Policy optimization candidate(s)** (0 occurrences)
  - **Duplicate Objects**
    - **Service** (1 occurrences)
    - **Application Control List** (1 occurrences)
    - **DLP Sensor** (1 occurrences)
    - **AV Profile** (1 occurrences)

ADOM revisions

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

To configure ADOM revisions, select the *ADOM Revisions* button on the Policy & Objects tab.

Figure 164:ADOM revisions



ADOM Revisions

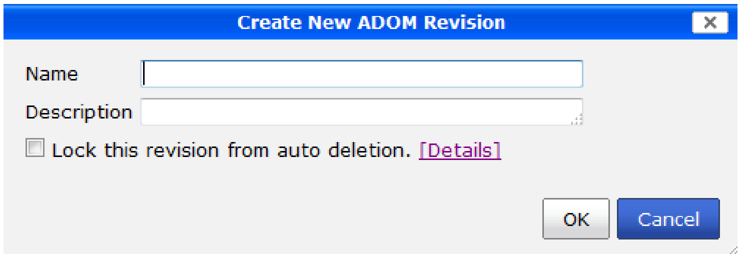
ID	Name	Created by	Creation Time	Comments
4	Restored-Tem2	admin	2013-03-15 09:18:34	Restored-The second one
3	Restored-Telemitry	admin	2013-03-15 09:18:23	Restored-uh...
2	Tem2	admin	2013-03-15 09:17:59	The second one
1	Telemitry	admin	2013-03-15 09:15:48	uh...

To add a new ADOM revision:

1. Go to the Policy & Objects tab and select the *ADOM Revisions* button in the toolbar. The *ADOM Revisions* window opens.
2. Right-click within the ADOM revisions table and select *New* in the pop-up menu.

   The *Create New ADOM Revision* dialog box opens.

   Figure 165: Create new ADOM revision

3. Enter a name for the revisions in the *Name* field.
4. Optionally, enter a description of the revision in the *Description* field.
5. To prevent the revision from being automatically deleted, select *Lock this revision from auto deletion*.
6. To configure the automatic deletion of revisions, select *[Details]*. See "To configure automatic deletion:" on page 221.
7. Select *OK* to create the new ADOM revision.

A new ADOM revision can only be created if changes have been made to that ADOM.

To edit an ADOM revision:

1. Open the *ADOM Revisions* window and either double-click on the revision, or right-click on the revision and select *Edit* from the pop-up menu.

   The *Edit ADOM Revision* dialog box opens.
2. Edit the revision details as required, then select *OK* to apply your changes.

To delete ADOM revisions:

1. Open the *ADOM Revisions* window.
2. To delete a single revision, right-click on the revision and select *Delete* from the pop-up menu.

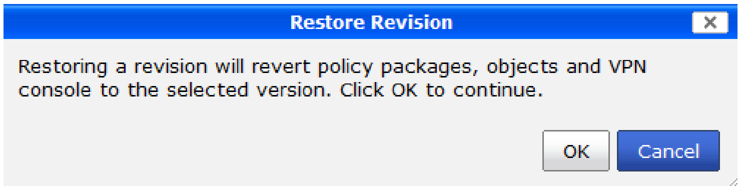
   To delete multiple revisions, use the Ctrl or Shift keys on your keyboard to select multiple revisions, or right-click on a revision and select Select All from the pop-up menu to select all of the revision. Then, right-click on any one of the selected revisions and select *Delete* from the pop-up menu.
3. Select *OK* in the confirmation dialog box to delete the selected revision or revisions.

To restore a revision:

1. Open the *ADOM Revisions* window.
2. Right-click on the revision to be restored and select *Restore* from the pop-up menu.

   If no changes have been made since the last revision was create, the *Restore Revision* window opens.

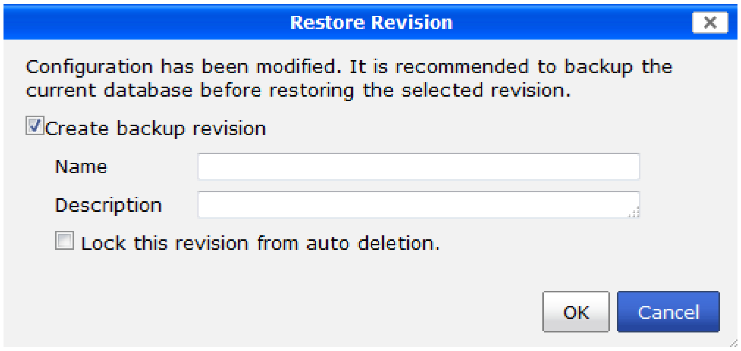
Figure 166: Restore revision



Restoring a revision will revert policy packages, objects and VPN console to the selected version. Click OK to continue.

If changes have been made to ADOM that have not been saved in a revision, the *Restore Revision* dialog box will present you with the option of creating a new revision prior to restoring the selected revision.

Figure 167: Restore and create a new revision



Configuration has been modified. It is recommended to backup the current database before restoring the selected revision.

☑ Create backup revision

Name

Description

□ Lock this revision from auto deletion.

3. If creating a new revision while restoring a previous revision, enter the required information into the *Restore Revision* dialog box.
4. Select *OK* to restore the revision.

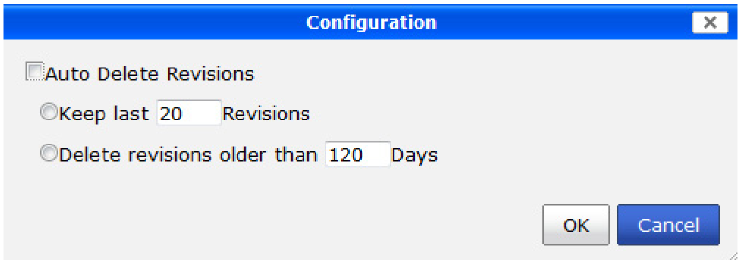
   The revision is restored and a new revision is created for the restored revision with the prefix *Restored-* appended to the original name of the revision.

To configure automatic deletion:

1. Open the *ADOM Revisions* window.
2. Right-click on any revision in the table and select *Edit* from the pop-up menu.
3. In the *Edit ADOM Revision* dialog box select *[Details]*.

   The *Configuration* dialog box opens.

Figure 168:ADOM revision deletion configuration



□ Auto Delete Revisions

○ Keep last 20 Revisions

○ Delete revisions older than 120 Days

4. To enable to automatic deletion of revisions, select *Auto Delete Revisions*.

5. Select one of the two available options for autmatic deletion of revisions:
   - *Keep last x Revisions*: Only keep the entered numbered of revisions, deleting the oldest revision when a new revision is created.
   - *Delete revision older than x Days*: Delete all revisions that are older than the entered number of days.
6. Select *OK* to apply the changes, then select *OK* again in the *Edit ADOM Revision* dialog box.

To lock or unlock an ADOM revision:

1. Open the *ADOM Revisions* window.
2. Do one of the following:
   - Right-click on a revision in the table and select *Lock* or *Unlock* from the pop-up menu.
   - Edit the revision and select or deselect *Lock this revision from auto deletion* from the *Edit ADOM Revision* dialog box. See "To edit an ADOM revision:" on page 220.

   The ADOM revision is locked.

About objects and dynamic objects

All objects within an ADOM are managed by a single database unique to that ADOM. Objects inside that database can include items such as addresses, services, intrusion protection definitions, antivirus signatures, web filtering profiles, etc.

When making changes to an object within the object database, changes are reflected immediately within the policy table in the Web-based Manager. No copying to the database is required.

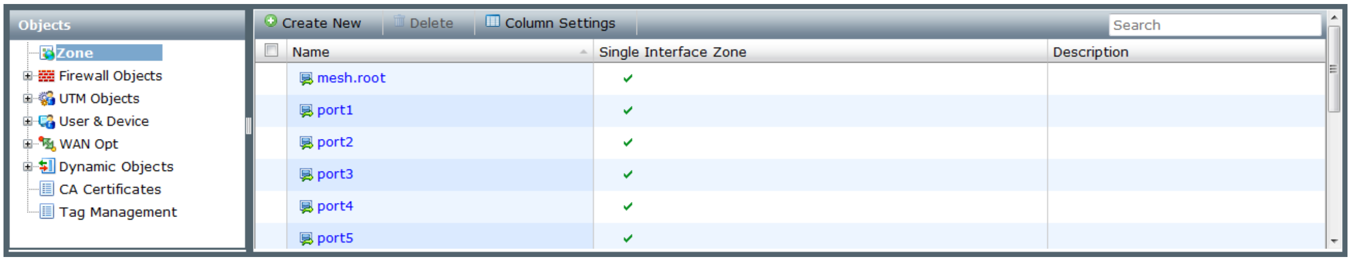
Dynamic objects are used to map a single logical object to a unique definition per device. Addresses, interfaces, virtual IPs, and an IP pool can all be addressed dynamically.

Not all policy and object options are enabled by default. To configure the enabled options, go to *System Settings* > *Admin* > *Admin Settings* and select your required options. See "Administrator settings" on page 90 for more information.

Managing objects and dynamic objects

Objects and dynamic objects are managed in lower frame of the *Policy & Objects* tab. The available objects varies depending on whether a specific ADOM or *Global* is selected.

Figure 169: Objects list



Name	Single Interface Zone	Description
mesh.root	✓	
port1	✓	
port2	✓	
port3	✓	
port4	✓	
port5	✓	

Objects can be dragged and dropped from the object frame into specific cells of a given policy. For example, an address object can be dragged into the source or destination cells of a policy. For more information see "Drag and drop objects" on page 226.

To view more information about an object in a policy, hover the pointer over the cell that contains that object. After one second, a tool tip will appear giving information about the object or objects in that cell.

Lock an ADOM

If workspace is enabled, you must lock an ADOM prior to performing any management tasks on it. See "Lock an ADOM" on page 214 for instructions.

Create a new object

To create a new object:

1. Select the specific ADOM in which you are creating the object from the drop-down list in the toolbar, or select *Global* to create a global object.

   The objects list is displayed in lower frame.

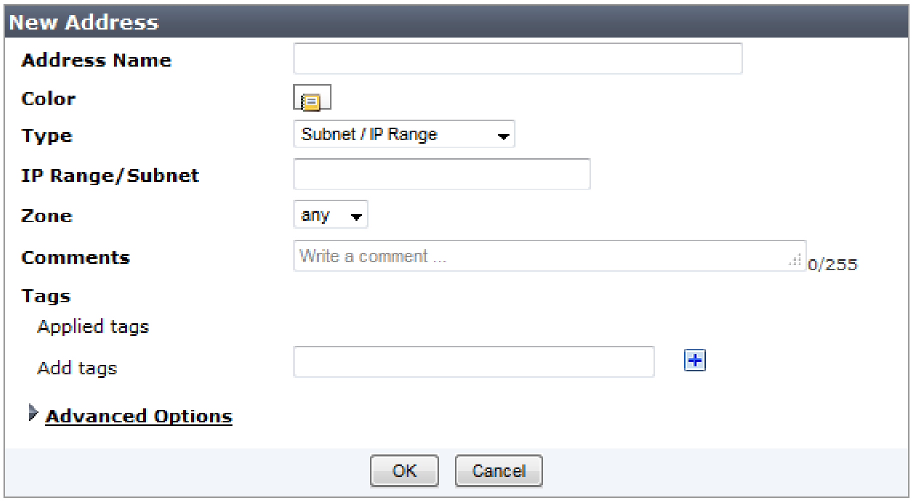
2. Select the object type that you will be creating. For example, view the firewall addresses by going to *Firewall Objects* > *Address*.

   The firewall address list is displayed in the lower content pane. The available address or address group lists are selectable on the lower content pane toolbar.

3. To create a new firewall address, select *Create New*, then select the type of address from the drop-down list. In this example, *Address* was selected.

4. The *New Address* dialog window will open.

Figure 170: Create new firewall address object



New Address

Address Name

Color

Type: Subnet / IP Range

IP Range/Subnet

Zone: any

Comments: Write a comment ... 0/255

Tags

Applied tags

Add tags

5. Enter the required information, depending on the object or object group selected, and then select *OK* to create the new object or object group.

Map a dynamic object

This example shows the basic steps for mapping an already created firewall address object. The same process is used for mapping other object types.

The devices and virtual domains to which a global object is mapped can also be viewed from the object list. See "To view dynamic object mappings:" on page 224.

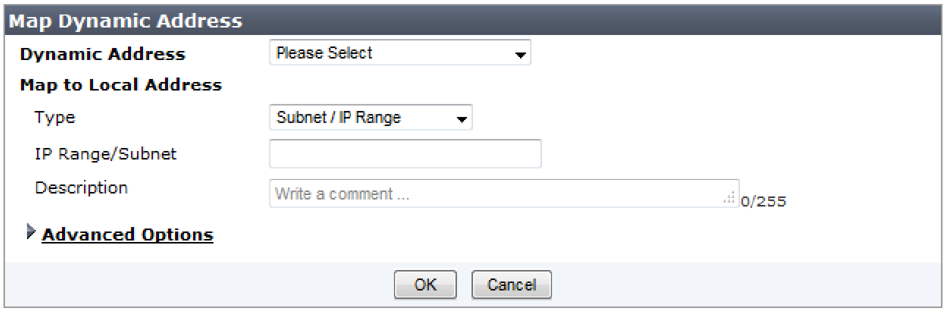
To map a dynamic object:

1. Go to the *Device Manager* tab, select the ADOM containing the device you want to map the dynamic object to, select the device type, such as *All FortiGate* or *All FortiSwitch*, and then select the device from the device list in the content frame.
2. From the toolbar in the lower right content frame, select *Address*.

   The *Map Dynamic Address* dialog box will open.

The *Address* tab is not available by default. To add it, select the plus symbol on the right side of the dashboard toolbar, then select *Address* in the *Dynamic Objects* section of the *Customize Tabs* dialog box. See “View managed devices” on page 121.

Figure 171: Map Dynamic Address dialog box



Map Dynamic Address

Dynamic Address: Please Select

Map to Local Address

Type: Subnet / IP Range

IP Range/Subnet:

Description: Write a comment ... 0/255

3. Select an address from the *Dynamic Address* drop-down list (which contains all the address objects you have created), then map that address to a local address.
4. Optionally, add a description of the local address and adjust any required advanced settings, and then select *OK* to map the dynamic address object.

To view dynamic object mappings:

1. Browse to the location of the object whose dynamic mappings you want to view in the object tree menu.
2. Right-click on the object in the object list and select *Dynamic Object Mappings*.

   The *Dynamic Object Mappings* dialog box opens, showing the details of the object and the devices and virtual domains to which it is mapped.
3. Select *OK* to close the dialog box.

Remove an object

To remove an object, browse to the object’s location in the object tree menu, select the object in the object list, and either click on the *Delete* button, or right-click on the object name and select *Delete* from the pop-up menu.

Edit an object

To edit an object:

1. Browse to the location of the object that you want to edit in the object tree menu.
2. From the object list in the lower content pane, do one of the following:
    - Double-click on the name of the object to be edited
    - Right-click on the name of the object to be edited and select *Edit* from the pop-up menu.
3. Edit the information as required, and select *OK*.

Clone an object

If a new object that you are creating is similar to a previously created object, the new object can be created by cloning the previous object.

To clone an object:

1. Browse to the location of the object that is to be cloned in the object tree menu.
2. Right-click on the object or group and select *Clone* from the pop-up menu.

   The *Edit* dialog box opens.
3. Adjust the information as required, and then select *OK* to create the new object.

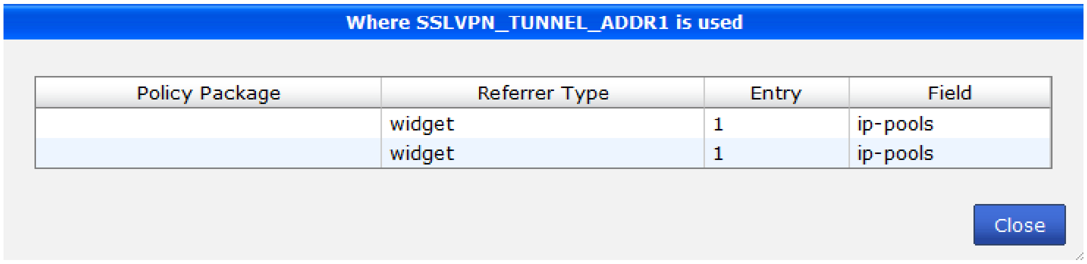
Search where an object is used

To determine where an object is being used:

1. Browse to the location of the object in the object tree menu.
2. Right-click on the object or group and select *Where Used* from the pop-up menu.

   The *Where Used* dialog box opens and displays the locations where the selected object is used; see Figure 172.

   Figure 172: Where Used dialog box



Where SSLVPN_TUNNEL_ADDR1 is used

Policy Package	Referrer Type	Entry	Field
	widget	1	ip-pools
	widget	1	ip-pools

3. Select *Close* to close the dialog box.

Search objects

The search objects tool allows you to search objects based on keywords.

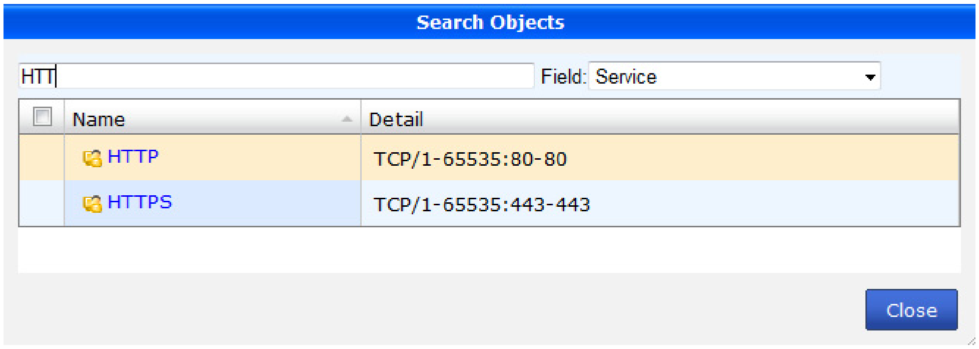
To dynamically search objects:

1. Browse to the object type that you would like to search in the object tree menu.
2. In the search box on the right side lower content frame toolbar enter a search keyword.
3. The results of the search are updated as you type and displayed in the object list.

To search objects:

1. In the *Policy & Objects* tab, right-click on any policy package and select *Search* from the pop-up menu.
2. The *Search Objects* dialog box opens.

Figure 173: Search Objects dialog box



□	Name	Detail
	HTTP	TCP/1-65535:80-80
	HTTPS	TCP/1-65535:443-443

3. Enter a search keyword and select the field you would like to search.
4. The results of the search are displayed in the dialog box.

Drag and drop objects

Objects can be dragged and dropped from the object frame into specific cells of a given policy. For example, an address object can be dragged into the source or destination cells of a policy.

One or more objects can be dragged at the same time. When dragging a single object a box beside the pointer will display the name of the object being dragged. When dragging multiple objects, the box beside the pointer will show a count of the number of objects that are being dragged.

The cells or columns that the object or objects can be dropped into will be highlighted in the policy package pane. After dropping the object or objects into a cell or column, the object will immediately appear in the cell as part of the policy, or in all the cells of that column.

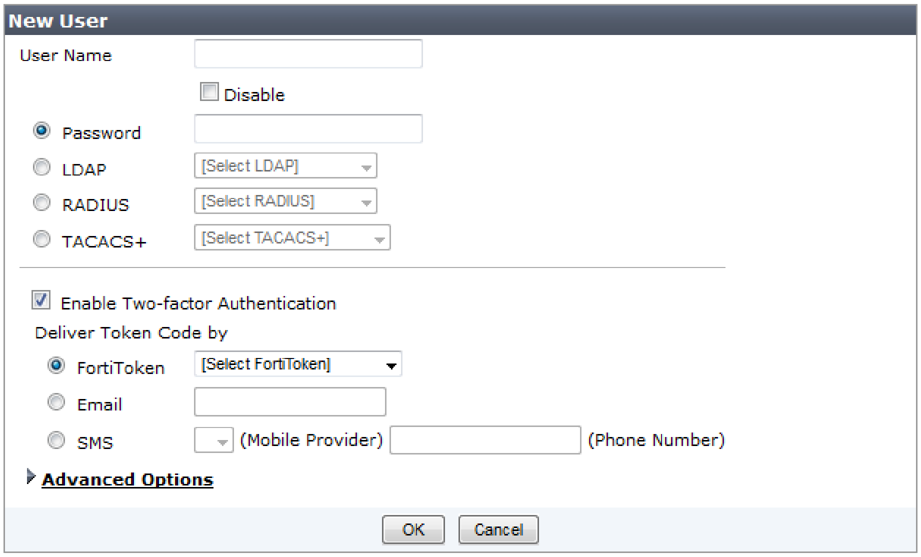
FortiToken configuration example

To configure FortiToken objects for FortiToken management, follow these steps:

1. In the object tree menu, browse to *User & Device* > *FortiToken*.
2. Select *Create New* from the lower content frame toolbar.
3. Enter the serial number or serial numbers of the FortiToken unit or units and select *OK* to save the setting.

   Up to ten serial numbers can be entered.
4. Browse to *User & Device* > *Local* to create a new user.
5. When creating the new user, select *Enable Two-factor Authentication,* and then select the FortiToken from the drop down menu.

Figure 174: New local user window



New User

User Name

□ Disable

● Password

○ LDAP [Select LDAP]

○ RADIUS [Select RADIUS]

○ TACACS+ [Select TACACS+]

☑ Enable Two-factor Authentication

Deliver Token Code by

● FortiToken [Select FortiToken]

○ Email

○ SMS (Mobile Provider) (Phone Number)

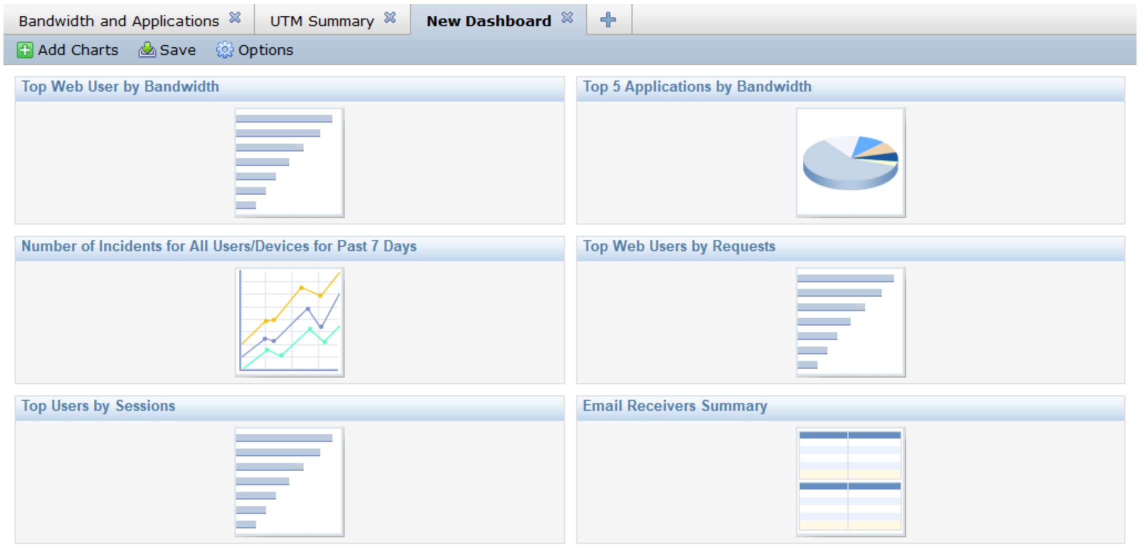
Advanced Options

6. Browse to *User & Device* > *User Group*, create a new user group, and add the previously created user to this group.
7. Install a policy package to the FortiGate, as described previously.
8. On the FortiGate, select *User* > *FortiToken*. Select the FortiToken created in Step 1 and select *OK* to activate the FortiToken unit.

RTM Profiles

The *RTM Profiles* tab allows you to create Real-Time Monitor (RTM) profiles and assign then them to one or more managed devices. Each profile contains one or more dashboards onto which various charts can be added, deleted, and arranged to display the desired real-time information. If ADOMs are enabled, RTM profiles are created within an ADOM, and can only be applied to devices within that ADOM. The real-time information can then be viewed in the device summary pane on the *Device Manager* tab.

Figure 175:RTM profiles tab


Bandwidth and Applications
UTM Summary
New Dashboard
Add Charts
Save
Options
Top Web User by Bandwidth
Top 5 Applications by Bandwidth
Number of Incidents for All Users/Devices for Past 7 Days
Top Web Users by Requests
Top Users by Sessions
Email Receivers Summary

RTM Profiles

RTM profiles contain one or more dashboards that consist of various predefined charts. A profile is assigned to one or more managed devices, and then the information defined by the selected charts in a given dashboard can be viewed in the device summary of the device to which the profile is assigned. See "View managed devices" on page 132 for more information.

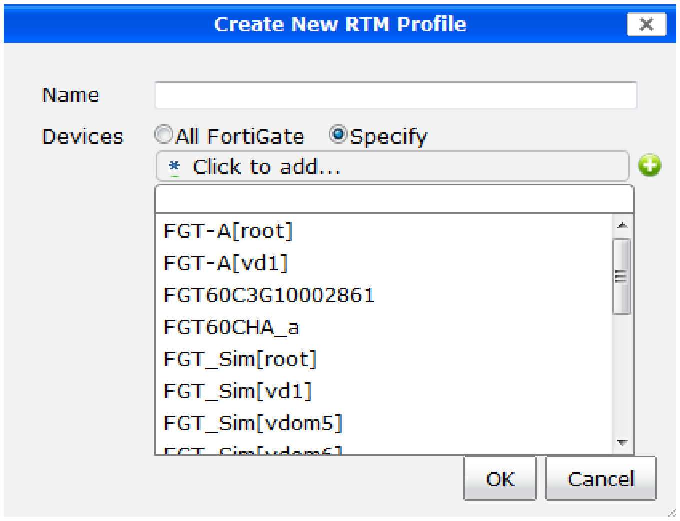
RTM profiles can be created, edited, cloned, and deleted. Cloning a profile allows you to create a second profile that is exactly the same as the original profile. This can save time when creating multiple profiles that only have slight differences.

To create a new RTM profile:

1. On the *RTM Profiles* tab, right click on a profile in the tree menu and select *Create New* from the pop-up menu.

   The *Create New RTM Profile* dialog box opens.

Figure 176: Create a new RTM profile



Name

Devices ○All FortiGate ●Specify

* Click to add...

FGT-A[root]
FGT-A[vd1]
FGT60C3G10002861
FGT60CHA_a
FGT_Sim[root]
FGT_Sim[vd1]
FGT_Sim[vdom5]
FGT_Sim[vdom6]

2. Enter a name for the profile in the *Name* field, and select the specific devices to which the profile will be assigned, or select *All FortiGate* to assign the profile to all FortiGate devices.

A device can only have a single RTM profile assigned to it. If a new profile is assigned to a device to which a profile has already been assigned, the newly assigned profile will displace the previously assigned profile.

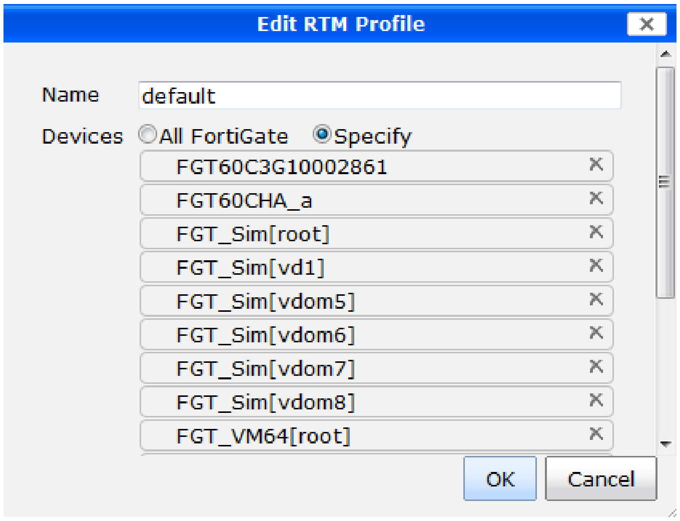
3. Select *OK* to create the new RTM profile.

To edit an RTM profile:

1. On the *RTM Profiles* tab, right click in the tree menu on the name of the profile you would like to edit, and select *Edit* from the pop-up menu.

   The *Edit RTM Profile* dialog box opens.

Figure 177: Edit an RTM profile



Name default

Devices ○All FortiGate ●Specify

FGT60C3G10002861 ✕
FGT60CHA_a ✕
FGT_Sim[root] ✕
FGT_Sim[vd1] ✕
FGT_Sim[vdom5] ✕
FGT_Sim[vdom6] ✕
FGT_Sim[vdom7] ✕
FGT_Sim[vdom8] ✕
FGT_VM64[root] ✕

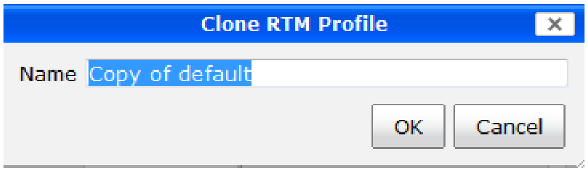
2. Edit the name of the profile and the devices to which the profile is assigned as needed, then select *OK* to finish editing the RTM profile.

To clone an RTM profile:

1. On the *RTM Profiles* tab, right click in the tree menu on the name of the profile you would like to clone, and select *Clone* from the pop-up menu.

   The *Clone RTM Profile* dialog box opens.

   Figure 178: Clone an RTM profile

   Name: Copy of default

2. Edit the name of the profile as needed, then select *OK* to finish cloning the RTM profile.

To delete an RTM profile:

1. On the *RTM Profiles* tab, right click in the tree menu on the name of the profile you would like to delete, and select *delete* from the pop-up menu.

   The *Delete RTM Profile* dialog box opens.

2. Select *OK* to delete the RTM profile.

Assigning RTM profiles to devices.

RTM profiles can be assigned to one or more managed devices that are in the same ADOM as the profile.

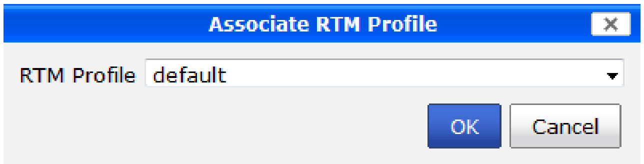
When creating a new RTM profile, it is assigned to a device or multiple devices. The assignment can also be changed by editing the RTM profile, or by selecting the profile from the *Configuration and Installation Status* widget on the device dashboard (see “Dashboard widgets” on page 126).

A device can only have a single RTM profile assigned to it. If a new profile is assigned to a device to which a profile has already been assigned, the newly assigned profile will displace the previously assigned profile.

To assign a profile to a device from the device dashboard:

1. On the *Device Manager* tab, select the ADOM or device group, for example *All FortiGates,* that contains the device in the tree-menu.
2. In the content pane, select the device whose RTM profile assignment you would like to change then locate the *Configuration and Installation Status* widget in the device dashboard.
3. In the *RTM Profile* field, select *[Change]* to open the *Associate RTM Profile* dialog box.

   Figure 179: Associate an RTM profile

   RTM Profile: default

4. Select an RTM profile from the drop-down list, or select *None* to have no RTM profile associated with the device, and then select *OK*.

Dashboards

Each RTM profile can contain multiple dashboards. A dashboard contains the charts that represent the information that will be presented in the device summary.

Each dashboard in a profile can be selected from the Real Time Monitor tab on the device summary toolbar. See “View managed devices” on page 132 for more information.

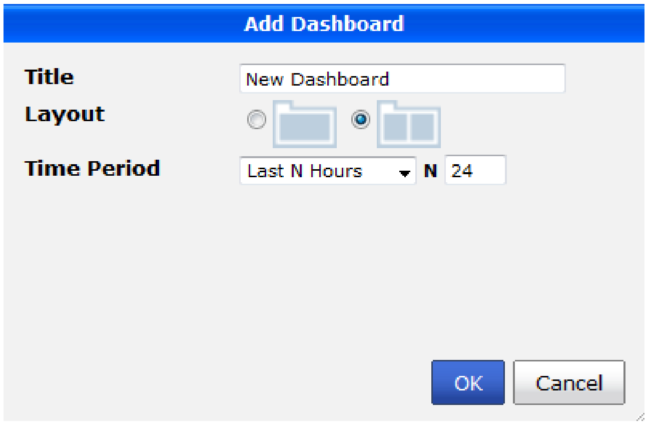
Dashboards can be created, edited, and deleted.

To create a new dashboard:

1. On the *RTM Profiles* tab, select the +, or *Add Dashboard*, icon in the content pane toolbar.

The *Add Dashboard* dialog box will open

Figure 180: Add dashboard dialog box



Title: New Dashboard

Layout: ○ ●

Time Period: Last N Hours N 24

2. Enter a name for the new dashboard in the *Title* field, select the number of columns the dashboard will contain (one or two) and enter the time period that the data in the charts will cover in the *Time Period* field.

The available time periods are:

Last 7 Days	Last N Hours	Last Quarter
Last 14 Days	Last N Days	This Year
Last 30 Days	Last N Weeks	Today
This Week	This Month	Yesterday
Last Week	Last Month	Other
Last 2 Weeks	This Quarter	

Where *N* represents a variable, allowing for a user selectable number of hours, days, or weeks.

If *Other* is selected, the start and end date and time must be manually entered.

3. Select *OK* to create the new dashboard.

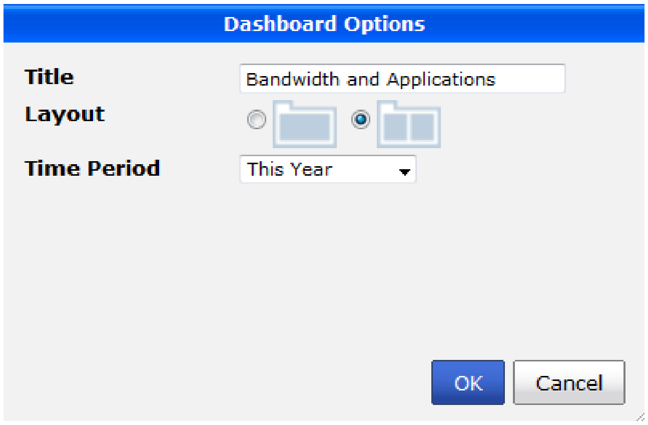
The new dashboard will appear on the content pane toolbar to the right of any previously created dashboards in that profile.

To edit a dashboard:

1. On the *RTM Profiles* tab, select the dashboard you would like to edit, and then select *Options*.

   The *Dashboard Options* dialog box will open

   Figure 181: Dashboard options dialog box

   Dashboard Options

   Title: Bandwidth and Applications

   Layout: ○ ●

   Time Period: This Year

2. Edit the dashboard information as required, then select *OK* to finish editing the dashboard.

To delete a dashboard:

1. On the *RTM Profiles* tab, select the *X*, or *Delete*, icon to the right of the in dashboard name for the dashboard that you would like to delete.
2. Select *OK* in the confirmation box to delete the dashboard and all of its data.

Charts

Charts are predefined to show specific information in an appropriate format, such as pie charts or lists. They are organized into categories, and can be added to, removed from, and organized on dashboards.

In a profile dashboard, the charts are shown as placeholders. When viewing the charts in the device summary (see “View managed devices” on page 132), they will be populated with real-time data.

The currently available predefined charts are outline in Table 12. New charts can also be created, see “Charts” on page 265 for more information

The available predefined charts may change. Please see the latest release notes for updated information.

Table 12: Available predefined charts

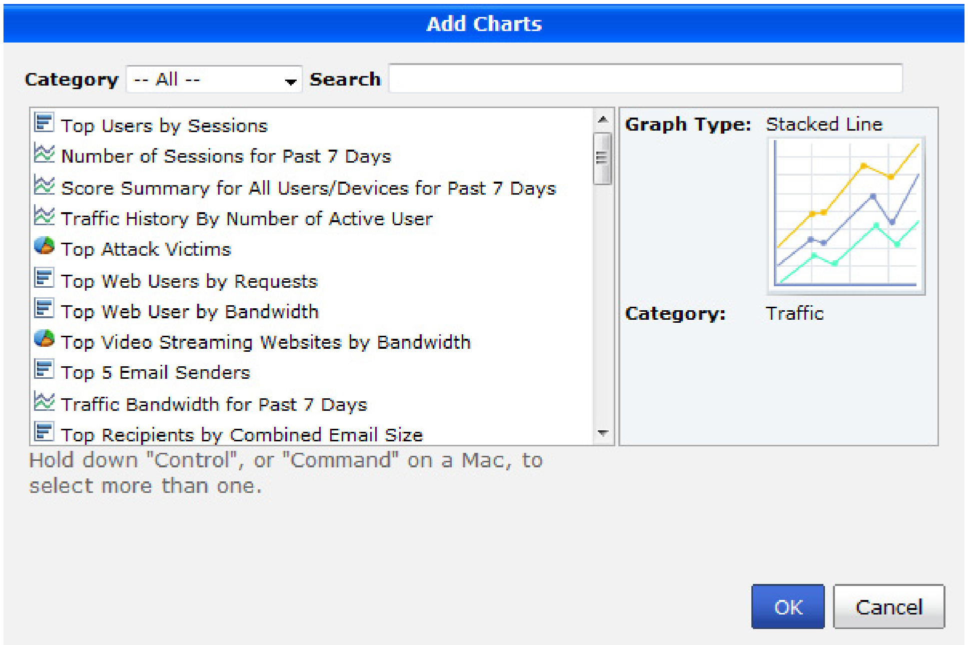
Event		
Top SSL-VPN Tunnel Users by Bandwidth	Top SSL-VPN Web Mode Users by Bandwidth	
IPS (Attack)		
Top Attack Victims	Top Attacks	Top Attack Source
Network Scan		
List Number of Vulnerabilities		
Traffic		
Top Users by Sessions	Number of Sessions for Past 7 Days	Score Summary for All Users/Devices for Past 7 Days
Traffic History by Number of Active User	Top 5 Email Senders	Traffic Bandwidth for Past 7 Days
Top Recipients by Combined Email size	Top Users with Increased Scores for Last 2 Periods	Top 5 Destinations
Top Site-to-Site IPsec Tunnels by Bandwidth	Top Destination Addresses by Sessions	Top 5 Applications by Sessions
Top 5 Applications by Bandwidth	Top Recipients by Number of Emails	Email Receivers Summary
Top 5 Email Recipients	Top Applications by Sessions	Top Destination Addresses by Bandwidth
Traffic Summary	Top Users by Bandwidth	Top 5 Users by Bandwidth
Top Senders by Number of Emails	Top Dial-Up IPsec Tunnels by Bandwidth	Number of Incidents for All Users/Devices for Past 7 Days
Top Applications by Bandwidth	Email Senders Summary	Top Users by Reputation Scores
Top Devices by Reputations Score	Top Devices with Increased Scored for Last 2 Periods	Top Senders by Combined Email Size
Virus		
Top Viruses by Name	Top Virus Victims	Top Viruses by Name
Web filter		
Top Web Users by Requests	Top Web User by Bandwidth	Top Video Streaming Websites by Bandwidth
Top 10 Allowed Sites	Top 10 Blocked Sites	Top Allowed Websites by Request
Top Blocked Websites	Top Blocked Users	Top Allowed Websites by Bandwidth

To add a chart to a dashboard:

1. In the *RTM Profiles* tab, select an RTM profile and the dashboard within that profile to which you would like to a add a chart.
2. Select *Add Charts* in the content pane toolbar.

   The *Add Charts* dialog box will open.

   Figure 182: Add charts dialog box



Add Charts

Category -- All -- Search

Top Users by Sessions
Number of Sessions for Past 7 Days
Score Summary for All Users/Devices for Past 7 Days
Traffic History By Number of Active User
Top Attack Victims
Top Web Users by Requests
Top Web User by Bandwidth
Top Video Streaming Websites by Bandwidth
Top 5 Email Senders
Traffic Bandwidth for Past 7 Days
Top Recipients by Combined Email Size

Graph Type: Stacked Line

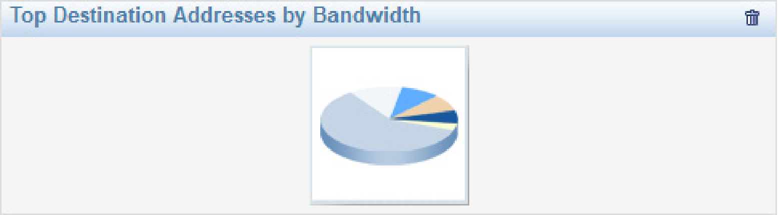
Category: Traffic

Hold down "Control", or "Command" on a Mac, to select more than one.

3. Find the chart that you would like to add in one of the following ways:
   - Browse the list of all the available the available charts.
   - Select the category of the chart you are looking for and then browse the list of the charts in that category.
   - Search for the chart by entering all or part of the chart name into the *Search* field.

   Once you select a chart, the graph type and the chart's category will be displayed in the preview box on the right of the dialog box.
4. Select *OK* to add the chart to the dashboard.

   Figure 183: Chart placeholder

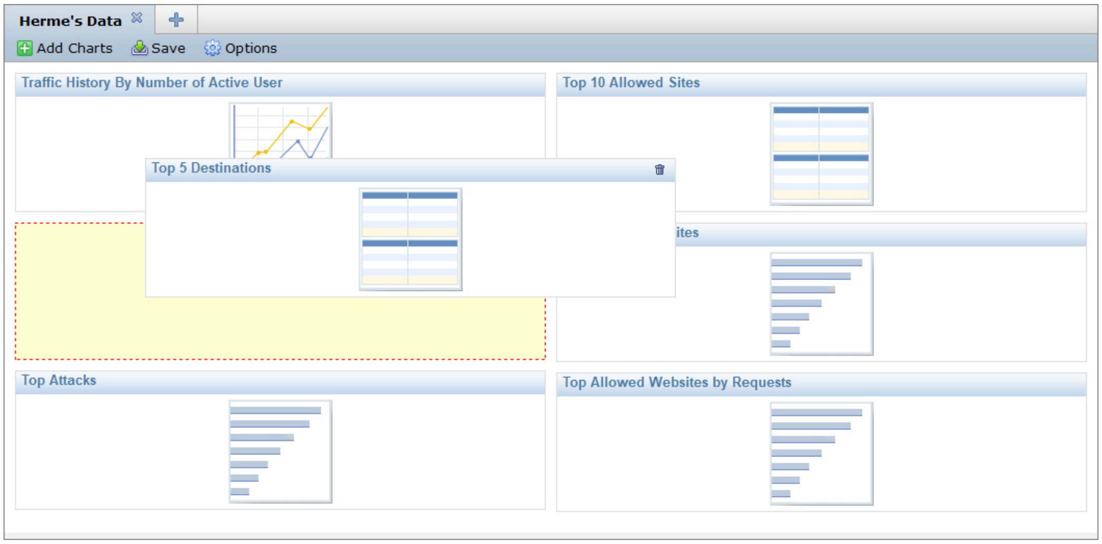


To reorganize the charts on a dashboard:

1. In the *RTM Profiles* tab, select an RTM profile and the dashboard within that profile that you would like to reorganize.
2. Click and drag any of the chart placeholders.

   The selected chart will follow the pointer so long as the left mouse button is held down. A yellow spacer with a dashed red outline will appear in the location where the chart will be once the mouse button is released.

   Figure 184: Moving a chart

3. Move the chart placeholder up, down, or to the side if the dashboard has two columns (see "To edit an RTM profile:" on page 229).
4. When the outlined yellow spacer box is in the location that you want the chart, release the mouse button and the chart will fall into place.
5. When you are finished reorganizing the dashboard, select the *Save* button in the content pane toolbar to save your changes.

To remove a chart from a dashboard:

1. In the *RTM Profiles* tab, select an RTM profile and the dashboard within that profile that contains the chart you would to remove.
2. Select the garbage can icon in the top right corner of the chart placeholder that you would like to remove.
3. Select *OK* in the confirmation dialog box to remove the chart from the dashboard.
4. When you have finished removing charts, select the *Save* button in the content pane toolbar to save your changes.

View RTM data

After creating an RTM profile, adding dashboards and charts to it, and assigning it to a device, the real-time data can be viewed in the device summaries of the devices to which the RTM profile was assigned.

To view the RTM data:

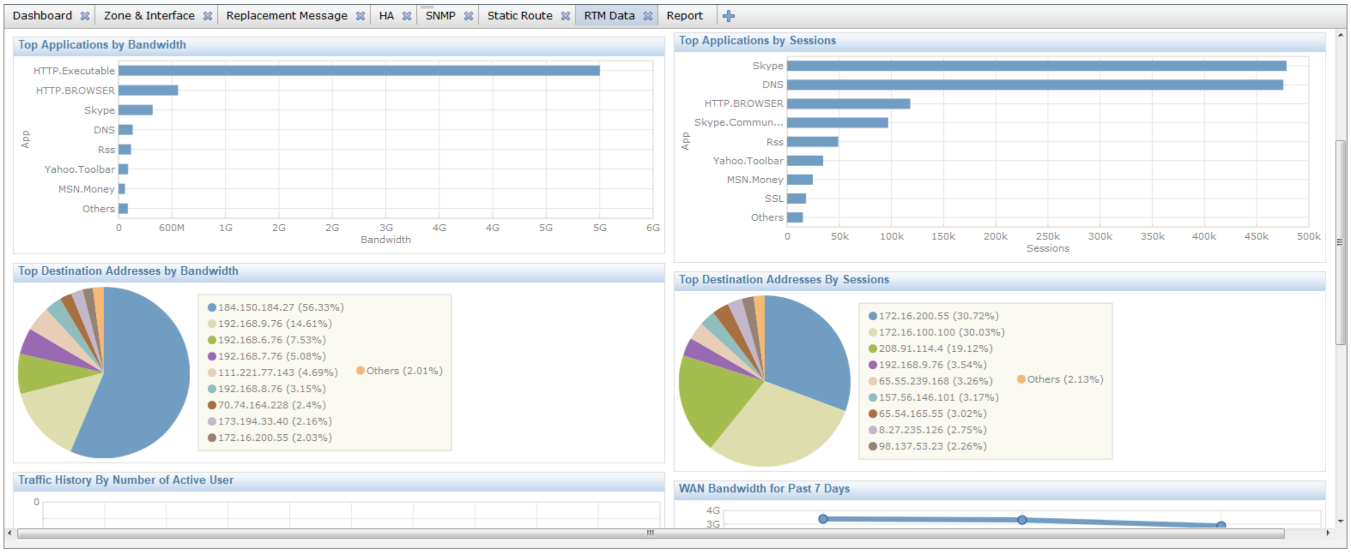
1. In the *Device Manager* tab, select the ADOM or group to which the device whose data you would like to view belongs.
2. From the device list in the content pane, select the desired device.

   The selected device’s dashboard will be shown in the lower content pane.
3. Select the RTM profile that you would like to view from device dashboard.

   By default, the RTM profiles will not be listed on the dashboard toolbar, see “View managed devices” on page 121 for instruction on adding the profiles to the toolbar.

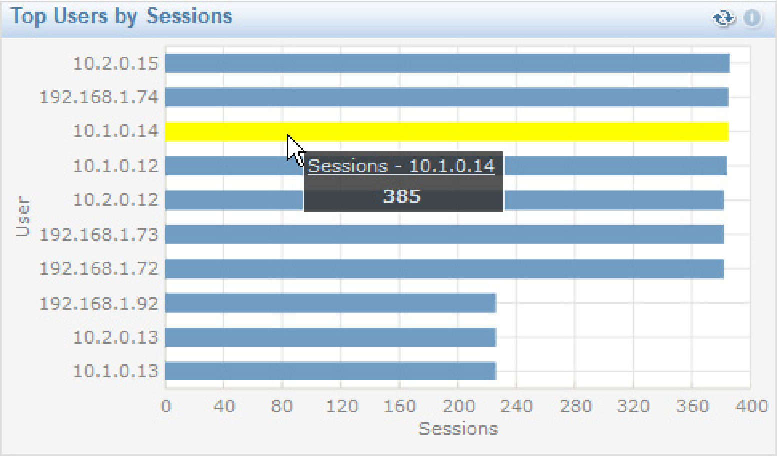
   The charts specified in the RTM profile dashboard will be populated with data and shown in the device summary pane.

Figure 185: Viewing RTM data



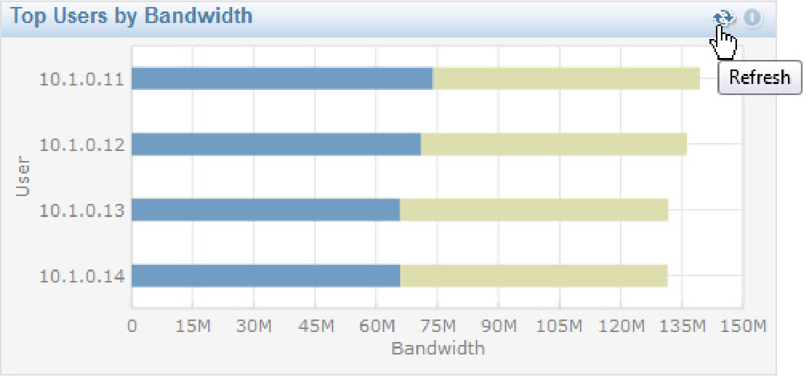
4. To view more detail on specific data within one of the charts, hover your cursor over a portion of the graph and a small dialog box will pop-up showing more data.

Figure 186: Chart data details



5. To refresh the data in a chart, select the Refresh button in the right corner of the chart title bar.

Figure 187: Refresh a chart's data



6. To make any changes to the layout of the charts, or to add or remove charts, return to the RTM Profile tab. For information see "RTM Profiles" on page 228, "Dashboards" on page 231, and "Charts" on page 232.

Log View

Logging and reporting can help you in determining what is happening on your network, as well as informing you of certain network activity, such as detection of a virus or IPsec VPN tunnel errors. Logging and reporting go hand in hand, and can become a valuable tool for information as well as helping to show others the activity that is happening on the network.

Your FortiManager device collects logs from managed FortiGate and FortiCarrier devices. You can view traffic logs, event logs, and UTM security logs.

Traffic logs record the traffic that is flowing through your FortiGate unit. Since traffic needs firewall policies to properly flow through the unit, this type of logging is also referred to as firewall policy logging. Firewall policies control all traffic that attempts to pass through the FortiGate unit, between FortiGate interfaces, zones and VLAN sub-interfaces.

The event log records administration management as well as FortiGate system activity, such as when a configuration has changed, admin login, or high availability (HA) events occur. Event logs are an important log file to record because they record FortiGate system activity, which provides valuable information about how your FortiGate unit is performing. The event logs includes *System*, *Router*, *VPN*, and *User* menu objects to provide you more granularity in viewing and searching log data.

UTM security logs record all antivirus, web filtering, application control, intrusion prevention, email filtering, data leak prevention, and VoIP activity on your managed devices.

For more information on logging see the *Logging and Reporting for FortiOS v5.0 Handbook* at http://docs.fortinet.com/fgt/handbook/50/fortigate-loggingreporting-50.pdf.

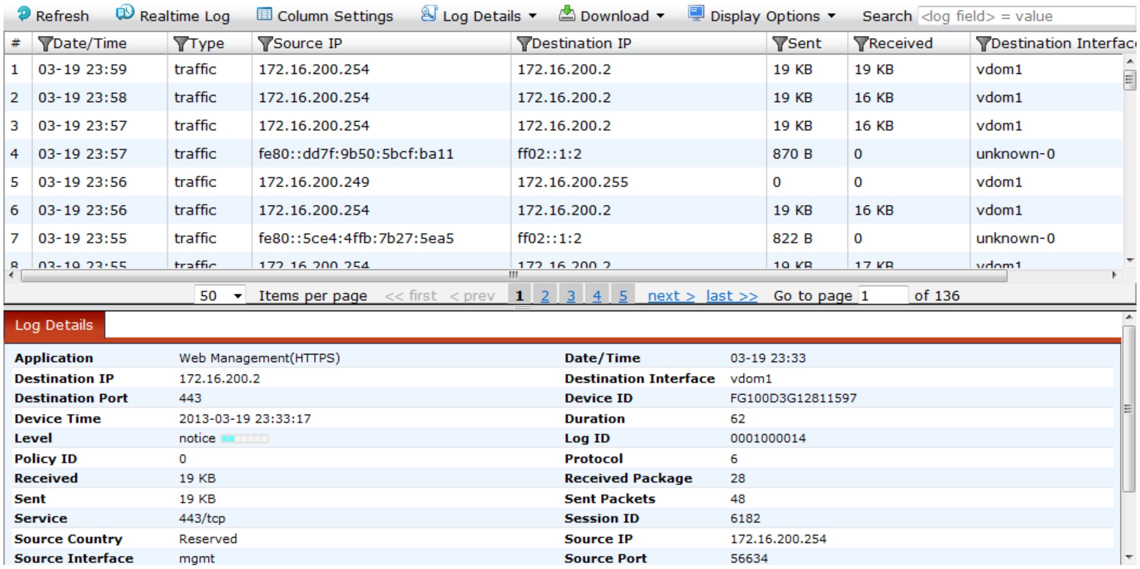
The *Log View* tab shows log messages for connected devices, organized by ADOMs. You can also view, import, and export log files stored for a given device.

FortiManager v5.0 Patch Release 2 introduces an *Alerts Viewer* menu object to configure log based alerts based on certain logging filters.

Viewing log messages

To view log messages, select the *Log View* tab and browse to the device whose logs you would like to view in the tree menu. You can view the traffic log, event log, or UTM security log information per device or per log array.

Figure 188: View logs



#	Date/Time	Type	Source IP	Destination IP	Sent	Received	Destination Interfac
1	03-19 23:59	traffic	172.16.200.254	172.16.200.2	19 KB	19 KB	vdom1
2	03-19 23:58	traffic	172.16.200.254	172.16.200.2	19 KB	16 KB	vdom1
3	03-19 23:57	traffic	172.16.200.254	172.16.200.2	19 KB	16 KB	vdom1
4	03-19 23:57	traffic	fe80::dd7f:9b50:5bcf:ba11	ff02::1:2	870 B	0	unknown-0
5	03-19 23:56	traffic	172.16.200.249	172.16.200.255	0	0	vdom1
6	03-19 23:56	traffic	172.16.200.254	172.16.200.2	19 KB	16 KB	vdom1
7	03-19 23:55	traffic	fe80::5ce4:4ffb:7b27:5ea5	ff02::1:2	822 B	0	unknown-0
8	03-19 23:55	traffic	172.16.200.254	172.16.200.2	19 KB	17 KB	vdom1

Log Details

Application	Web Management(HTTPS)	**Date/Time**	03-19 23:33
Destination IP	172.16.200.2	**Destination Interface**	vdom1
Destination Port	443	**Device ID**	FG100D3G12811597
Device Time	2013-03-19 23:33:17	**Duration**	62
Level	notice	**Log ID**	0001000014
Policy ID	0	**Protocol**	6
Received	19 KB	**Received Package**	28
Sent	19 KB	**Sent Packets**	48
Service	443/tcp	**Session ID**	6182
Source Country	Reserved	**Source IP**	172.16.200.254
Source Interface	mgmt	**Source Port**	56634

Refresh	Refresh the log view.
Real time Log	Select to view real time logs. Only available when *Historical Log* has been selected.
Historical Log	Select to view historical logs. Only available when *Real time Log* has been selected.
Column Settings	Select to change the columns to view and the order they appear on the page.
Log Details	Adjust the location and visibility of the *Log Details* frame. It can be hidden, or visible on the bottom or right side of the content pane. For more information, see "Log details" on page 242.
Download	Select to download the logs. Two options are available: • *Current View*: Select to download log files in text (.txt), or comma-separated value (.csv). The downloaded version will match the current log view, containing only log messages that match your current filter settings. • *Raw Log*: Select to download log files in text (.txt), or comma-separated value (.csv) for a specified date and time range.
Pause/Resume	Pause and resume real time log display. Only available when *Real time Log* has been selected.
Display Options	Select to change the log display options. Select between *Formatted* (default) and *Raw*.

Search	Enter a value in the search field to search the listed logs.
Date/Time	The date and time the log was received by the FortiManager unit.
Other	Other columns will be available, depending on the log type selected in the tree menu.
Pages	Settings to adjust the number of logs listed per page and to browse through the pages of logs.
Log Details frame	Detailed information on the log message selected in the log message list. See “Log details” on page 242 for more information.

Depending on configuration and the device, different logs will be available, such as traffic logs, various event logs, and others.

Customizing the log view

The columns in the log message list can be customized to show only relevant information in your preferred order.

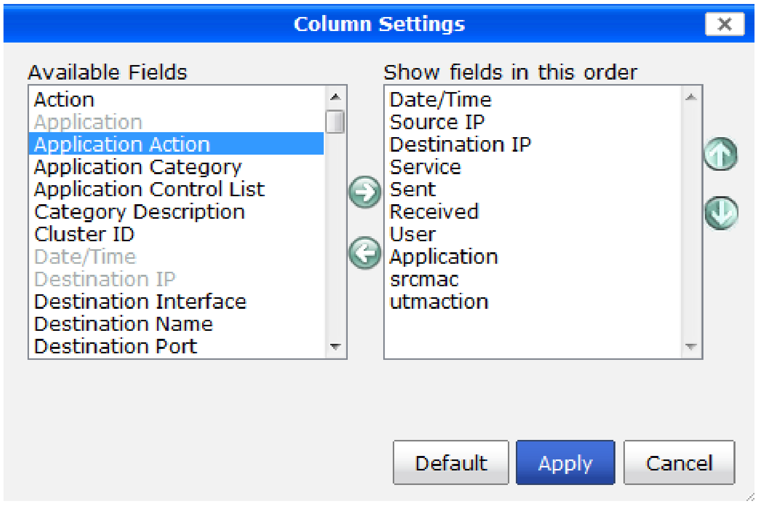
For most columns, you can also filter data within the columns to include or exclude log messages which contain your specified text in that column. Most column headings contain a gray filter icon, which becomes green when a filter is configured and enabled.

To display or hide columns:

1. Browse to the log message list you would like to customize
2. Select *Column Settings* in the toolbar.

   The *Column Settings* dialog box opens.

   Figure 189: Column settings dialog box

3. Select which columns to hide or display.
   - In the *Available Fields* area, select the names of individual columns you want to display, then select the single right arrow to move them to the *Show fields in this order* area.
   - In the *Show fields in this order* area, select the names of individual columns you want to hide, then select the single left arrow to move them to the *Available Fields* area.
   - To return all columns to their default displayed/hidden status, select *Default*.

4. Select *Apply* to apply the changes to the log message list.

To change the order of the columns:

1. Browse to the log message list you would like to customize
2. Select *Column Settings* in the toolbar.

   The *Column Settings* dialog box opens.
3. In the *Show fields in this order* area, select a column name whose order of appearance you want to change.
4. Select the up or down arrow to move the column in the ordered list.

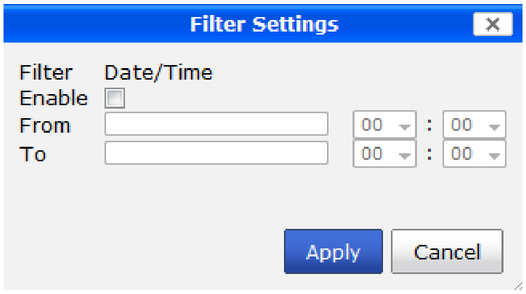
   Placing a column name towards the top of the *Show fields in this order* list will move the column to the left side of the log message list.
5. Select *Apply* to apply the changes to the log message list.

To filter log messages by column content:

1. In the heading of the column that you want to filter, select the filter icon to open the *Filter Settings* dialog box for that column.

   The Filter Settings dialog boxes are specific to the column you are filtering.

   Figure 190: Date/Time filter settings dialog box



Filter Date/Time

Enable □

From 00 : 00

To 00 : 00

2. Enter the requisite information to filter the selected column and then select *Apply*.

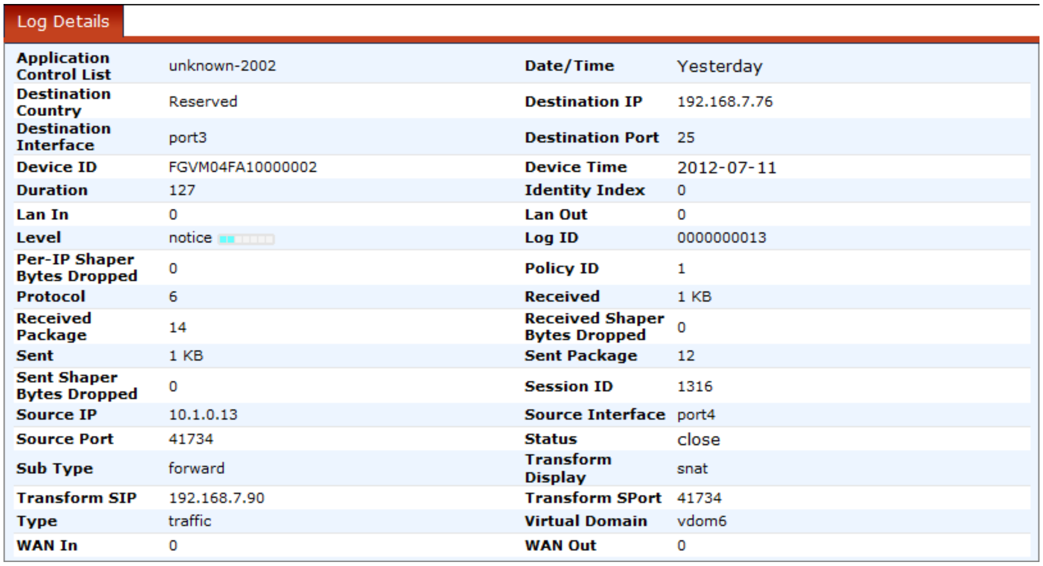
   The column’s filter icon will turn green when the filter is enabled. Downloading the current view will only download the log messages that meet the current filter criteria.

Log details

Log details can be viewed for any of the collected logs.

To view log details, select the log in the log message list. The log details will be displayed in the lower frame of the content pane.

Figure 191: Log details



Application Control List	unknown-2002	**Date/Time**	Yesterday
Destination Country	Reserved	**Destination IP**	192.168.7.76
Destination Interface	port3	**Destination Port**	25
Device ID	FGVM04FA10000002	**Device Time**	2012-07-11
Duration	127	**Identity Index**	0
Lan In	0	**Lan Out**	0
Level	notice	**Log ID**	0000000013
Per-IP Shaper Bytes Dropped	0	**Policy ID**	1
Protocol	6	**Received**	1 KB
Received Package	14	**Received Shaper Bytes Dropped**	0
Sent	1 KB	**Sent Package**	12
Sent Shaper Bytes Dropped	0	**Session ID**	1316
Source IP	10.1.0.13	**Source Interface**	port4
Source Port	41734	**Status**	close
Sub Type	forward	**Transform Display**	snat
Transform SIP	192.168.7.90	**Transform SPort**	41734
Type	traffic	**Virtual Domain**	vdom6
WAN In	0	**WAN Out**	0

The details provided in the log detail frame will vary depending on the type of log selected.

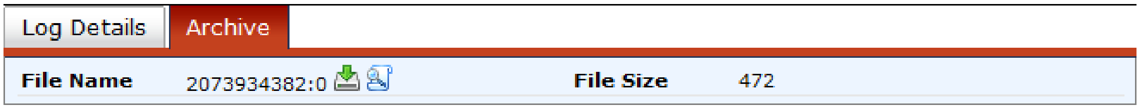
To adjust the location of the *Log Details* frame, select Log Details in the toolbar. From the drop-down list, select one of the following:

- ***On Right***: The *Log Details* frame will be shown on the right side of the screen.
- ***On Bottom***: The *Log Details* frame will be shown on the bottom of the content pane (default setting).
- ***Hidden***: The *Log Details* frame will be hidden from view.

Archive

The *Archive* tab is displayed next to the *Log Details* tab on the details frame when archived logs are available.

Figure 192: Log archives

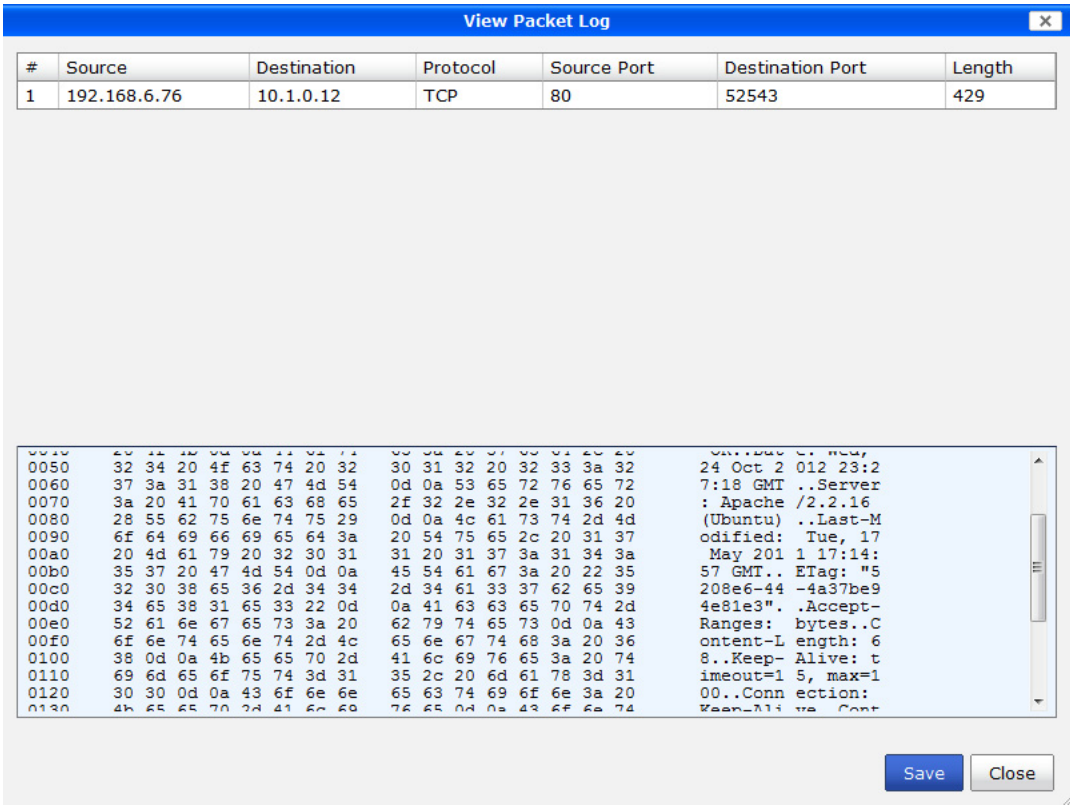


File Name	2073934382:0	**File Size**	472

The name and size of the archived log files are listed in the table. Selecting the download button next to the file name allows you to save the file to your computer.

Depending on the file type of the archived log file, the *View Packet Log* button may also be available next to the download button. Select this button to open the *View Packet Log* dialog box, which displays the path and content of the log file.

Figure 193: View packet log dialog box



#	Source	Destination	Protocol	Source Port	Destination Port	Length
1	192.168.6.76	10.1.0.12	TCP	80	52543	429

```
0050    32 34 20 4f 63 74 20 32   30 31 32 20 32 33 3a 32    24 Oct 2 012 23:2
0060    37 3a 31 38 20 47 4d 54   0d 0a 53 65 72 76 65 72    7:18 GMT ..Server
0070    3a 20 41 70 61 63 68 65   2f 32 2e 32 2e 31 36 20    : Apache /2.2.16
0080    28 55 62 75 6e 74 75 29   0d 0a 4c 61 73 74 2d 4d    (Ubuntu) ..Last-M
0090    6f 64 69 66 69 65 64 3a   20 54 75 65 2c 20 31 37    odified:  Tue, 17
00a0    20 4d 61 79 20 32 30 31   31 20 31 37 3a 31 34 3a     May 201 1 17:14:
00b0    35 37 20 47 4d 54 0d 0a   45 54 61 67 3a 20 22 35    57 GMT.. ETag: "5
00c0    32 30 38 65 36 2d 34 34   2d 34 61 33 37 62 65 39    208e6-44 -4a37be9
00d0    34 65 38 31 65 33 22 0d   0a 41 63 63 65 70 74 2d    4e81e3". .Accept-
00e0    52 61 6e 67 65 73 3a 20   62 79 74 65 73 0d 0a 43    Ranges:  bytes..C
00f0    6f 6e 74 65 6e 74 2d 4c   65 6e 67 74 68 3a 20 36    ontent-L ength: 6
0100    38 0d 0a 4b 65 65 70 2d   41 6c 69 76 65 3a 20 74    8..Keep- Alive: t
0110    69 6d 65 6f 75 74 3d 31   35 2c 20 6d 61 78 3d 31    imeout=1 5, max=1
0120    30 30 0d 0a 43 6f 6e 6e   65 63 74 69 6f 6e 3a 20    00..Conn ection:
0130    4b 65 65 70 2d 41 6c 69   76 65 0d 0a 43 6f 6e 74    Keep-Ali ve..Cont
```

Browsing log files

Log View > *[ADOM name]* > *Log Browse* displays log files stored for devices.

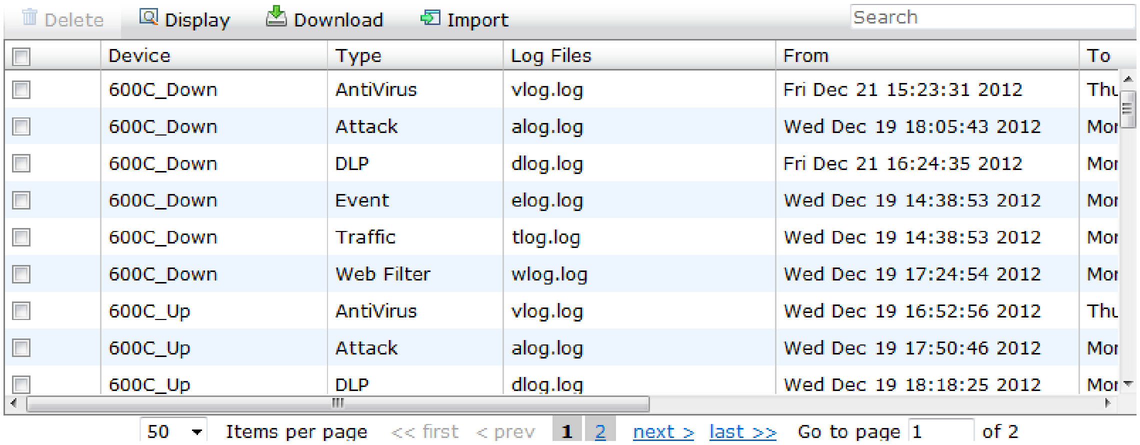
When a log file reaches its maximum size, or reaches the scheduled time, the FortiManager rolls the active log file by renaming the file. The file name will be in the form of xlog.N.log, where x is a letter indicating the log type and N is a unique number corresponding to the time the first log entry was received.

For information about setting the maximum file size and log rolling options, see “Configuring rolling and uploading of device logs” on page 246.

If you display the log messages in Formatted view, you can display and arrange columns and/or filter log messages by column contents. For more information, see “Customizing the log view” on page 240.

For more information about log messages, see the *FortiManager Log Message Reference*.

Figure 194: Log file list



☐	Device	Type	Log Files	From	To
☐	600C_Down	AntiVirus	vlog.log	Fri Dec 21 15:23:31 2012	Thu
☐	600C_Down	Attack	alog.log	Wed Dec 19 18:05:43 2012	Mor
☐	600C_Down	DLP	dlog.log	Fri Dec 21 16:24:35 2012	Mor
☐	600C_Down	Event	elog.log	Wed Dec 19 14:38:53 2012	Mor
☐	600C_Down	Traffic	tlog.log	Wed Dec 19 14:38:53 2012	Mor
☐	600C_Down	Web Filter	wlog.log	Wed Dec 19 17:24:54 2012	Mor
☐	600C_Up	AntiVirus	vlog.log	Wed Dec 19 16:52:56 2012	Thu
☐	600C_Up	Attack	alog.log	Wed Dec 19 17:50:46 2012	Mor
☐	600C_Up	DLP	dlog.log	Wed Dec 19 18:18:25 2012	Mor

50 Items per page << first < prev 1 2 next > last >> Go to page 1 of 2

This page displays the following:

Delete	Mark the check box of the file whose log messages you want to delete, then select this button.
Display	Mark the check box of the file whose log messages you want to view, then select this button. For more information, see "Viewing log messages" on page 239
Download	Mark the check box of the log file that you want to download, select this button, then select a format for saving the log files: text (.txt), or comma-separated value (.csv). For more information, see "Downloading a log file" on page 246.
Import	Select to import log files. For more information about importing log files, see "Importing a log file" on page 245.
Search	Search the log files by entering a text value in the search window. For example, search log files by device serial number.
Columns	
Device	The device host name.
Type	The log type.
Log Files	A list of available log files for each device or device group. Select the group name to expand the list of devices within the group, and to view their log files. The current, or active, log file appears as well as rolled log files. Rolled log files include a number in the file name, such as `vlog.1267852112.log`. If you configure the FortiManager unit to delete the original log files after uploading rolled logs to an FTP server, only the current log will exist.
From	The start time when the log file was generated.

To	The end time when the log file was generated.
Size (bytes)	The size of the log file.
Items per page	Select to display 50, 100, or 500 log items per page.
Got to page	Browse log file pages.

Importing a log file

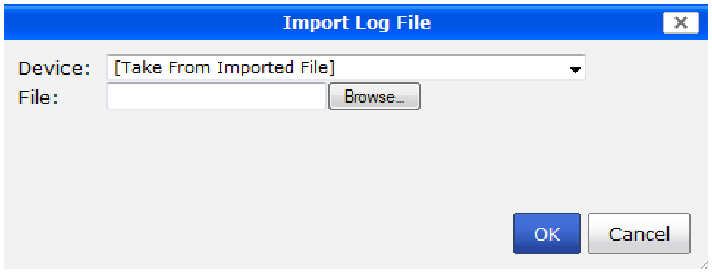
Importing a device's log files can be useful when restoring data, or loading log data for temporary use.

For example, if you have older log files from a device, you can import these logs to the FortiManager unit so that you can generate reports containing older data. Importing log files is also useful when changing your RAID configuration. Changing your RAID configuration reformats the hard disk, erasing log files. If you back up the log files, after changing the RAID configuration, you can import logs to restore them to the FortiManager unit.

To import a log file:

1. Go to *Log View* > *[ADOM name]* > *Log Browse*.
2. Select *Import*.

   Figure 195: Import a log file

   Import Log File

   Device: [Take From Imported File]

   File:

3. Select the device to which the imported log file belongs from the *Device* field drop-down list, or select *[Take From Imported File]* to read the device ID from the log file.

   If you select *[Take From Imported File]* your log file must contain a `device_id` field in its log messages.
4. In the *File* field, enter the path and file name of the log file, or select *Browse*. and browse to the log file.
5. Select *OK*.

   A message appears, stating that the upload is beginning, but will be cancelled if you leave the page.
6. Select *OK*.

   The upload time varies depending on the size of the file and the speed of the connection.

After the log file successfully uploads, the FortiManager unit inspects the log file.

- If the `device_id` field in the uploaded log file does not match the device, the import will fail. Select *Return* to attempt another import.
- If you selected *[Take From Imported File]*, and the FortiManager unit's device list does not currently contain that device, a message appears after the upload. Select *OK* to import the log file and automatically add the device to the device list, or select *Cancel*.

Downloading a log file

You can download a log file to save it as a backup or for use outside the FortiManager unit. The download consists of either the entire log file, or a partial log file, as selected by your current log view filter settings and, if downloading a raw file, the time span specified.

To download a whole log file:

1. Go to *Log View* > *[ADOM name]* > *Log Browse*.
2. Select the specific log file (wlog.log, elog.log, etc.) that you want to download.
3. Select *Download*.
4. If prompted by your web browser, select a location to where save the file, or open the file without saving, then select *OK*.

To download a partial log file:

1. Go to *Log View* > *[ADOM name]* > *Log Browse*.
2. Select the specific log file that you want to download.
3. Select *Display*.
4. Select a filter icon to restrict the current view to only items which match your criteria, then select *OK*.

   Filtered columns have a green filter icon. For more information about filtering log views, see "Customizing the log view" on page 240
5. Select *Download* and select either *Current View* or *Raw Log* from the drop-down list.
6. Select the log file format, either a text file or a csv file, and if desired select *Compress with gzip* to compress the log file.

   If you are downloading a raw log, you can specify the start and end dates for the data that you would like the file to include.
7. Select *Apply*.

   If prompted by your web browser, select a location to where save the file, or open the file without saving.

FortiClient logs

The FortiAnalyzer can receive FortiClient logs uploaded through TCP port 514. The FortiClient logs can be viewed and downloaded from *Log View* > *FortiClient*. For more information, see the *FortiClient v5.0 Patch Release 2 Administration Guide*.

Configuring rolling and uploading of device logs

You can control device's log file size and consumption of the FortiManager's disk space by configuring log rolling and scheduled uploads to a server.

As the FortiManager unit receives new log items, it performs the following tasks:

- verifies whether the log file has exceeded its file size limit
- checks to see if it is time to roll the log file if the file size is not exceeded.

Configure the time to be either a daily or weekly occurrence, and when the roll occurs. When a current log file (`tlog.log`) reaches its maximum size, or reaches the scheduled time, the FortiManager unit rolls the active log file by renaming the file. The file name will be in the form of `xlog.N.log` (for example, `tlog,1252929496.log`), where `x` is a letter indicating the log type and N is a unique number corresponding to the time the first log entry was received. The file modification time will match the time when the last log was received in the log file.

Once the current log file is rolled into a numbered log file, it will not be changed. New logs will be stored in the new current log called tlog.log. If log uploading is enabled, once logs are uploaded to the remote server or downloaded via the Web-based Manager, they are in the following format:

```
FG3K6A3406600001-tlog.1252929496.log-2012-09-29-08-03-54.gz
```

If you have enabled log uploading, you can choose to automatically delete the rolled log file after uploading, thereby freeing the amount of disk space used by rolled log files. If the log upload fails, such as when the FTP server is unavailable, the logs are uploaded during the next scheduled upload.

To enable and configure log rolling or uploading, go to *System Settings* > *Advanced* > *Device Log* > *Log Setting*. For more information, see "Log Setting" on page 111.

Alerts viewer

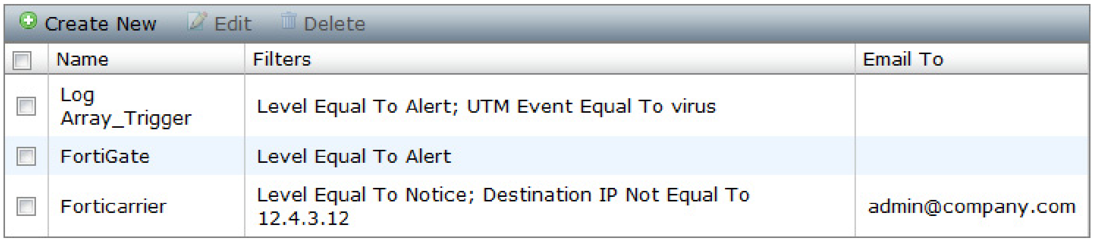
You can configure log based alerts based on certain logging filters. You can select to send the alert to an email address, SNMP server, or syslog server. Alerts can be configured per device or per log array.

Alerts can also be monitored and the logs associated with a given alert can be viewed.

Alert triggers

Go to *Log View* > *Alerts Viewer* > *Config* to view the configured alert triggers.

Figure 196: Alerts viewer page



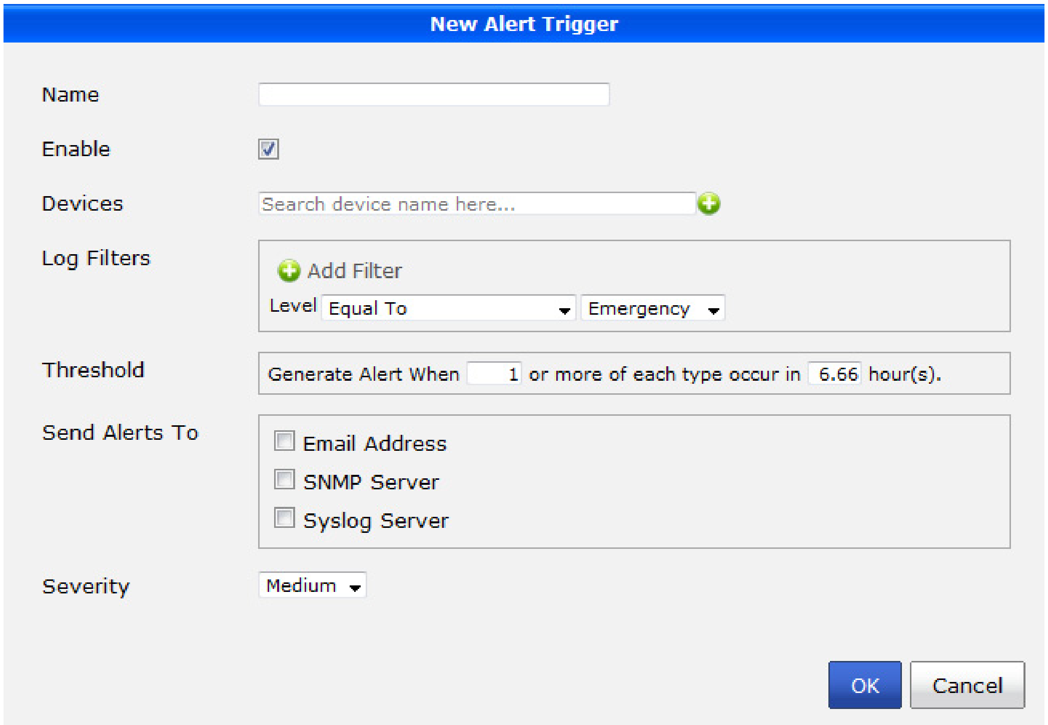
□	Name	Filters	Email To
□	Log Array_Trigger	Level Equal To Alert; UTM Event Equal To virus	
□	FortiGate	Level Equal To Alert	
□	Forticarrier	Level Equal To Notice; Destination IP Not Equal To 12.4.3.12	admin@company.com

To create a new alert trigger:

1. Go to *Log View* > *Alerts Viewer* > *Config*.
2. Select *Create New* in the tool-bar.

   The *New Alert Trigger* dialog box opens.

Figure 197: New alert trigger dialog box



New Alert Trigger

Name

Enable ☑

Devices: Search device name here...

Log Filters: Add Filter
Level: Equal To, Emergency

Threshold: Generate Alert When 1 or more of each type occur in 6.66 hour(s).

Send Alerts To:
□ Email Address
□ SNMP Server
□ Syslog Server

Severity: Medium

3. Configure the following settings:

Name	Enter a name for the alert trigger.
Enable	Select the checkbox to enable the alert trigger.
Devices	Select the plus (+) symbol to add devices or log arrays.
Log Filters	Select the plus (+) symbol to add log filters.
Level	Select the filter level in the first drop-down menu. Select the severity level in the second drop-down menu. Select one of the following: *Debug, Information*, *Notification*, *Warning*, *Error*, *Critical*, *Alert*, or *Emergency*.
Destination IP	Select to filter based on the destination IP, then enter an IP value in the text box.
Destination Port	Select to filter based on the destination port, then enter a port value in the text box.
Status	Select to filter based on the status, then select one of the following in the second drop-down menu: *DENY, ACCEPT, START, DNS, IP-CONN, WEB, CLOSE, TIMEOUT*.
UTM Event	Select to filter based on a UTM event, then enter a value in the text box.

Threshold	Generate Alert When ‘x’ or more of each type occur in ‘x’ hour(s).
Send Alerts To	
Email Address	Select the checkbox to enable. Enter a text value in the *To* and *From* text boxes and select the email server on the drop-down menu.
SNMP Server	Select the checkbox to enable. Select an SNMP server on the drop-down menu.
Syslog Server	Select the checkbox to enable. Select a syslog server on the drop-down menu.
Severity	Select the severity from the drop-down list.

4. Select *OK* to save the configuration.

To edit an alert trigger:

1. Go to *Log View* > *Alerts Viewer* > *Config*.

2. Select an alert trigger and select *Edit* in the tool-bar.

The *Edit Alert Trigger* dialog box opens.

3. Edit the settings as required.

4. Select *OK* to save the configuration.

To delete an alert trigger:

1. Go to *Log View* > *Alerts Viewer* > *Config*.

2. Select an alert trigger and select *Delete* in the tool-bar.

The confirmation pop-up window opens.

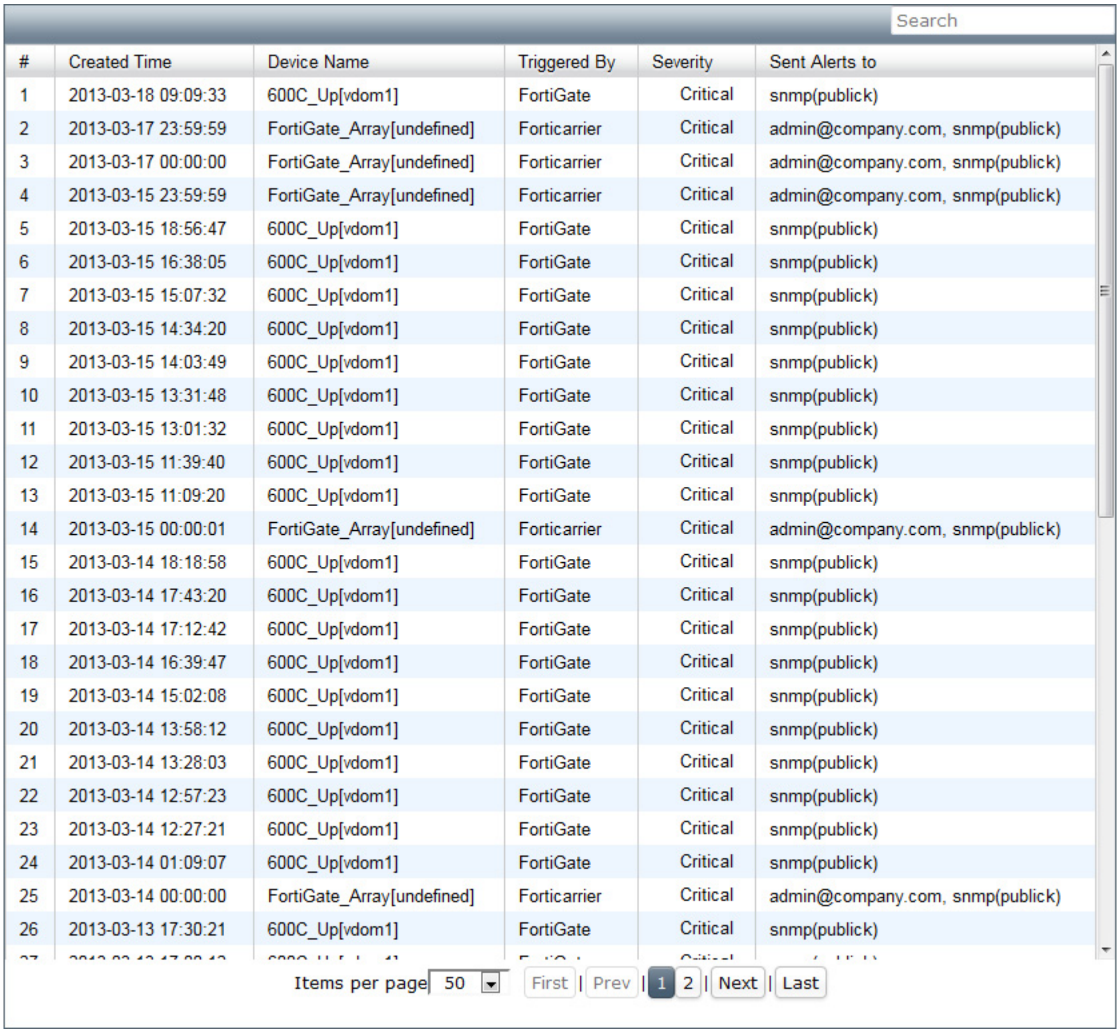
3. Select *OK* to proceed.

Alert monitor

The alert monitor provides al ist of the generated alerts. Right-clicking on an alert in the table gives you the option of viewing the log messages associated with that alert and acknowledging the alert.

To monitor alerts, go to *Log View* > *Alerts Viewer* > *Monitor*.

Figure 198: Monitor alerts

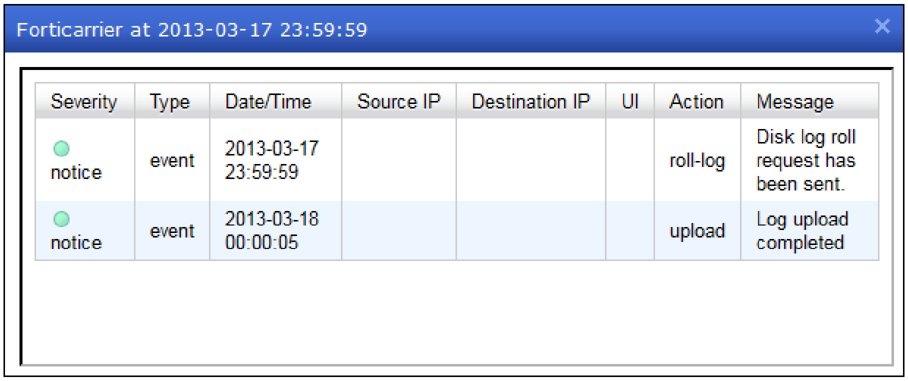


#	Created Time	Device Name	Triggered By	Severity	Sent Alerts to
1	2013-03-18 09:09:33	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
2	2013-03-17 23:59:59	FortiGate_Array[undefined]	Forticarrier	Critical	admin@company.com, snmp(publick)
3	2013-03-17 00:00:00	FortiGate_Array[undefined]	Forticarrier	Critical	admin@company.com, snmp(publick)
4	2013-03-15 23:59:59	FortiGate_Array[undefined]	Forticarrier	Critical	admin@company.com, snmp(publick)
5	2013-03-15 18:56:47	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
6	2013-03-15 16:38:05	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
7	2013-03-15 15:07:32	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
8	2013-03-15 14:34:20	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
9	2013-03-15 14:03:49	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
10	2013-03-15 13:31:48	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
11	2013-03-15 13:01:32	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
12	2013-03-15 11:39:40	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
13	2013-03-15 11:09:20	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
14	2013-03-15 00:00:01	FortiGate_Array[undefined]	Forticarrier	Critical	admin@company.com, snmp(publick)
15	2013-03-14 18:18:58	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
16	2013-03-14 17:43:20	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
17	2013-03-14 17:12:42	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
18	2013-03-14 16:39:47	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
19	2013-03-14 15:02:08	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
20	2013-03-14 13:58:12	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
21	2013-03-14 13:28:03	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
22	2013-03-14 12:57:23	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
23	2013-03-14 12:27:21	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
24	2013-03-14 01:09:07	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)
25	2013-03-14 00:00:00	FortiGate_Array[undefined]	Forticarrier	Critical	admin@company.com, snmp(publick)
26	2013-03-13 17:30:21	600C_Up[vdom1]	FortiGate	Critical	snmp(publick)

To view log messages associated with an alert:

1. Go to *Log View* > *Alerts Viewer* > *Monitor* and select the alert whose logs you would like to view.
2. Right-click and select *View Logs* from the pop-up menu.

Figure 199: View alert log messages



Forticarrier at 2013-03-17 23:59:59

Severity	Type	Date/Time	Source IP	Destination IP	UI	Action	Message
● notice	event	2013-03-17 23:59:59				roll-log	Disk log roll request has been sent.
● notice	event	2013-03-18 00:00:05				upload	Log upload completed

3. Close the dialog box to return to the alerts table.

To acknowledge alerts:

1. Go to *Log View* > *Alerts Viewer* > *Monitor* and select the alert or alerts you would like to acknowledge.
2. Right-click and select *Acknowledge* from the pop-up menu.
3. Select OK in the confirmation dialog box to acknowledge the selected alert or alerts.

Reports

FortiManager units can analyze information collected from the log files of connected devices. It then presents the information in tabular and graphical reports. These reports provide a quick and detailed analysis of activity on your networks.

To reduce the number of reports needed, reports are independent from devices, and contain layout information in the form of a report template. The devices, groups, and any other required data related information can be added as parameters to the report at the time of report generation.

Additional configuration options and short-cuts are available using the right-click menu. Right-click the mouse on different navigation panes on the Web-based Manager page to access these options.

The *Reports* tab allows you to configure reports using the pre-defined report templates, configure report schedules, view report history and the report calendar, and configure and view charts, datasets, and output profiles.

This chapter contains the following sections:

- Templates
- Schedules
- History
- Calendar
- Advanced

If ADOMs are enabled. each ADOM will have its own report settings.

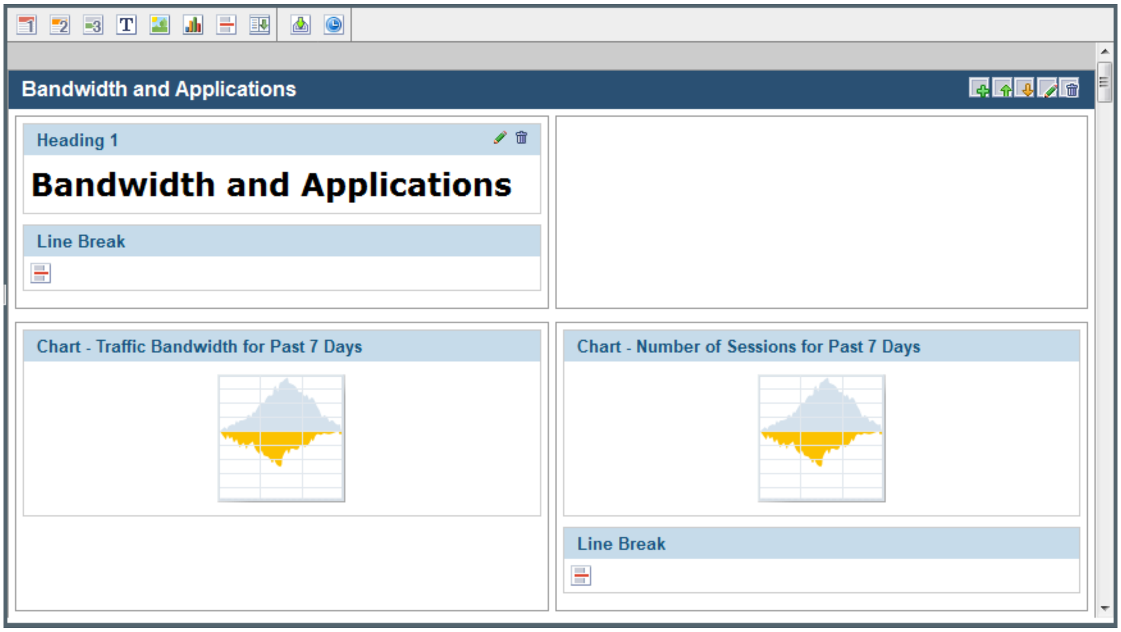
Templates

The FortiManager has two pre-configured report template: Client Reputations, and UTM Security Analysis. This template can be used as is, and you can also clone or edit the template. You can create template folders to help organize your templates, and new templates that can be customized as required.

The Client Reputation report template reports user and device reputation scores.

The UTM Security Analysis report template reports popular bandwidth and application log data. The template consists of various charts organized under different headings.

Figure 200: Report templates


Bandwidth and Applications
Heading 1
Bandwidth and Applications
Line Break
Chart - Traffic Bandwidth for Past 7 Days
Chart - Number of Sessions for Past 7 Days
Line Break

Configure report templates

Report templates can be created, edited, cloned, deleted, and organized into folders. New content can be added to and organized on a template, including: new sections, three levels of headings, text boxes, images, charts, and line and page breaks.

To create a new report template:

1. Go to the *Reports* tab and right-click on *Report Templates* in the tree menu.
2. In the right-click menu, under the *Template* heading, select *Create New*.
3. In the *Create New Report Template* dialog box, enter a name for the template, and select *OK*.

   A new template with a single, blank section is created with the given name.

To clone a report template:

1. Go to the *Reports* tab and right-click on the report you would like to clone in the tree menu.
2. In the right-click menu, under the *Template* heading, select *Clone*.
3. In the *Clone Report Template* dialog box, enter a name for the new template, and select *OK*.

   A new template with the same information as the original template is created with the given name.

To create a new report template folder:

1. Go to the *Reports* tab and right-click on *Report Templates* in the tree menu.
2. In the right-click menu, under the *Folder* heading, select *Create New*.
3. In the *Create New Folder* dialog box, enter a name for the folder, and select *OK*.

   A new template folder is created with the given name.

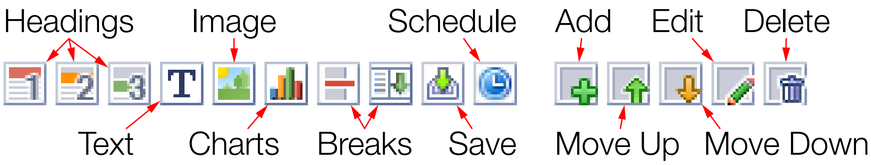
To delete a report template or report template folder:

1. Go to the *Reports* tab and right-click on the report template or report template folder that you would like to delete in the tree menu.
2. In the right-click menu select *Delete*.
3. In the confirmation dialog box, select *OK* to delete the report template or folder.

Add report template content

Various content can be added to a report template, such as charts, images, and typographic elements, using the section and template toolbars.

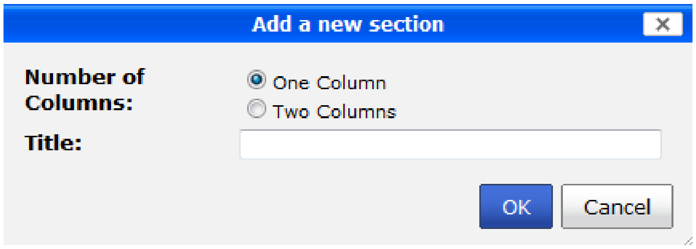
Figure 201: Template and section toolbars



To add a section to a report template:

1. Go to the *Reports* tab and select the template from the tree menu to which you would like to add content.
2. From the section toolbar, select the *Add* icon.
3. The *Add a new section* dialog box opens.

   Figure 202: Add a new section



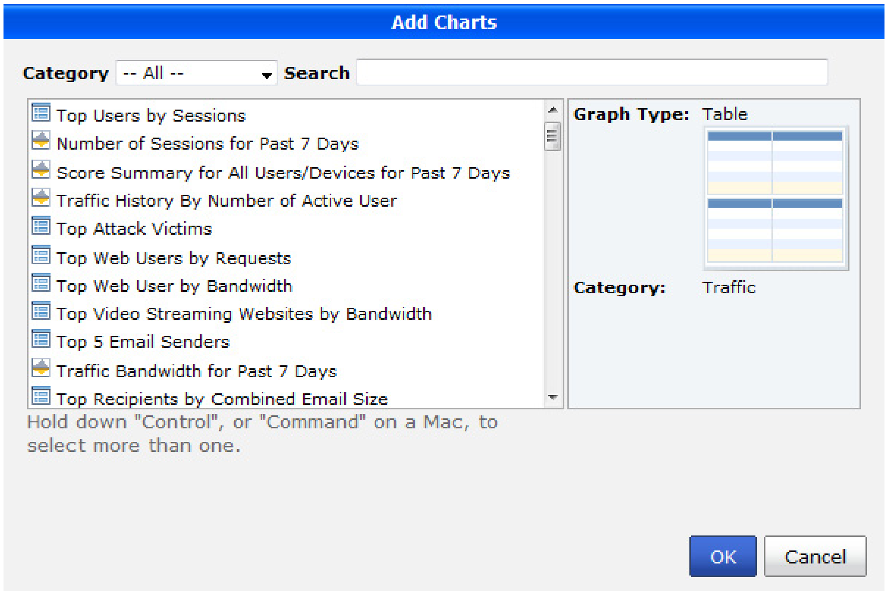
4. Select the number of columns that the section will contain, either one or two, and enter a title for the section.
5. Select *OK* to create the new section.
6. If you are finished editing the template, select the *Save* icon to save your changes.

To add a chart to a report template:

1. Go to the *Reports* tab and select the template from the tree menu to which you would like to add a chart.
2. Click and drag the chart icon to the location where you want to add the chart.

   When you release the mouse button, the *Add a New Chart* dialog box will open.

Figure 203: Add a new chart


Add Charts

Category -- All -- Search

- Top Users by Sessions
- Number of Sessions for Past 7 Days
- Score Summary for All Users/Devices for Past 7 Days
- Traffic History By Number of Active User
- Top Attack Victims
- Top Web Users by Requests
- Top Web User by Bandwidth
- Top Video Streaming Websites by Bandwidth
- Top 5 Email Senders
- Traffic Bandwidth for Past 7 Days
- Top Recipients by Combined Email Size

Hold down "Control", or "Command" on a Mac, to select more than one.

Graph Type: Table

Category: Traffic

3. Find the chart that you would like to add in one of the following ways:
   - Browse the list of all the available the available charts.
   - Select the category of the chart you are looking for and then browse the list of the charts in that category.
   - Search for the chart by entering all or part of the chart name into the *Search* field.
4. Select *OK* once you have selected the chart you would like to add.

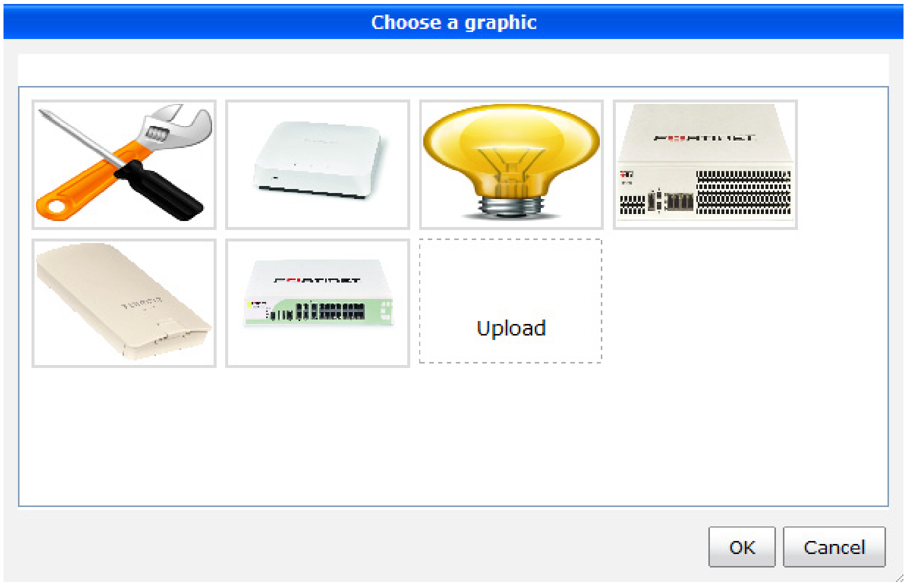
   The chart's placeholder will appear in the location that you had selected in the template.
5. If you are finished editing the template, select the *Save* icon to save your changes.

To add an image to a report template:

1. Go to the *Reports* tab and select the template from the tree menu to which you would like to add an image.
2. Click and drag the image icon to the location where you want to add the image.

   The *Choose a graphic* dialog box will open.

Figure 204: Choose a graphic



3. Select an image from the list, or select *Upload* to browse for an image on your computer.
4. Select *OK* once you have selected the image you would like to add.

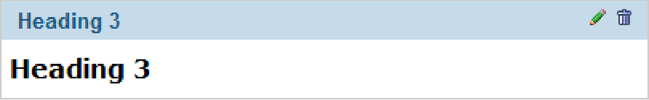
   The image will appear in the location that you had selected in the template.
5. If you are finished editing the template, select the *Save* icon to save your changes.

To add headings to a report template:

1. Go to the *Reports* tab and select the template from the tree menu to which you would like to add headings.
2. Click and drag the required heading icon to the location where you want to add the template heading.

   When you release the mouse button, the selected element will be placed into the template.

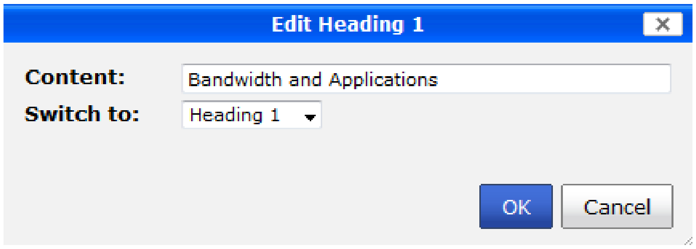
Figure 205: Heading element



3. To edit the heading text and level, select the edit icon on the template element, or double-click on the element.

   The *Edit Heading* dialog box will open.

Figure 206: Edit a heading



Content: Bandwidth and Applications

Switch to: Heading 1

4. Enter the heading text in the *Content* field and, if necessary, change the heading level with the *Switch to* drop-down list.

5. Select *OK* to finish editing the heading.
6. If you are finished editing the template, select the *Save* icon to save your changes.

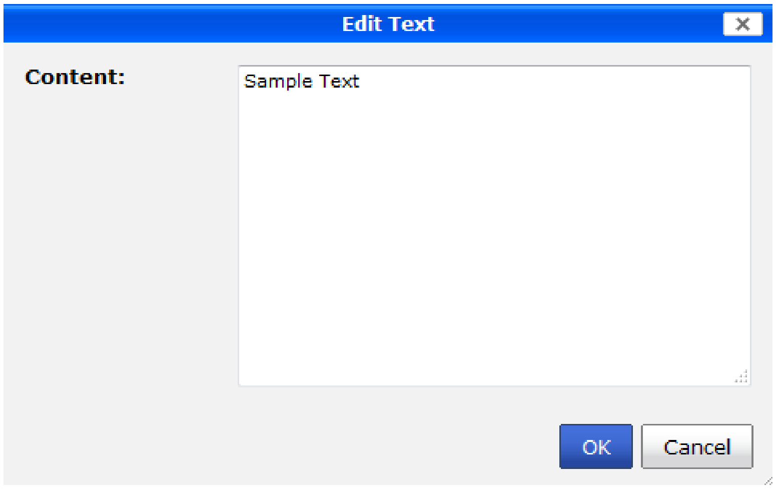
To add text to a report template:

1. Go to the *Reports* tab and select the template from the tree menu to which you would like to add text.
2. Click and drag the text icon to the location where you want to add the text box.

   When you release the mouse button, the selected element will be placed into the template.
3. To edit the text, select the edit icon on the template element, or double-click on the element.

   The *Edit Text* dialog box will open.

Figure 207: Edit text



Sample Text

4. Enter the text in the *Content* field.
5. Select *OK* to finish editing the text.
6. If you are finished editing the template, select the *Save* icon to save your changes.

To add breaks to a report template:

1. Go to the *Reports* tab and select the template from the tree menu that you would like to edit.
2. Click and drag the required break icon to the location where you want to add the break. Line breaks and page breaks are available.

   When you release the mouse button, the selected break will be placed into the template.
3. If you are finished editing the template, select the *Save* icon to save your changes.

Edit report template content

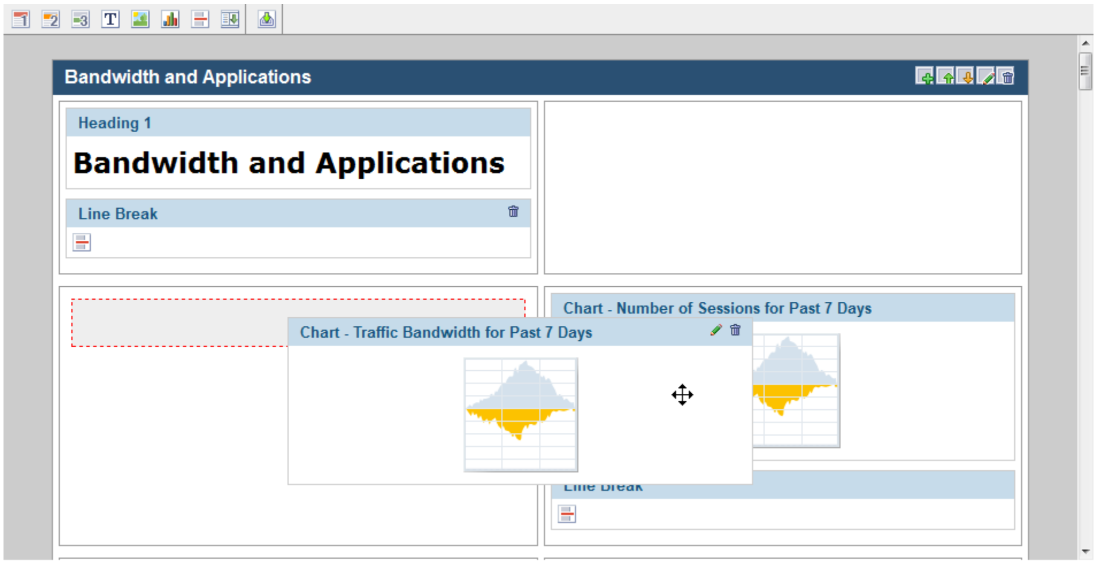
The elements added to report template can be moved, deleted, and some of them can be edited.

To move a report template element:

1. Go to the *Reports* tab and select the template from the tree menu that you would like to edit.
2. Click and drag an element to the desired location.

   A gray box with a dashed red outline will appear in the location where the element will be placed.
3. Release the mouse button to drop the element into the desired location.

Figure 208: Move a report template element

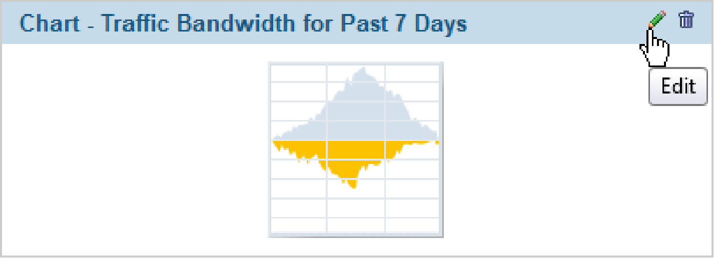

Bandwidth and Applications
Heading 1
Bandwidth and Applications
Line Break
Chart - Traffic Bandwidth for Past 7 Days
Chart - Number of Sessions for Past 7 Days
Line Break

4. When you are finished editing the template, select the *Save* icon to save your changes.

To edit a report template element:

1. Go to the *Reports* tab and select the template from the tree menu that contains to the element you would like to edit.
2. Select the edit icon in top right corner of the element to be edited. Break elements cannot be edited.

Figure 209: Edit an element



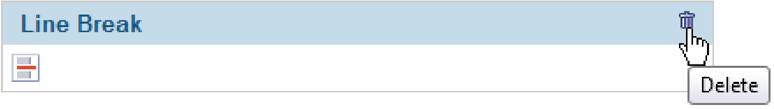
3. Depending on the type of element you are editing, an appropriate edit dialog box will open.

   The edit element dialog boxes contain the same information as the add element dialog boxes, see “Add report template content” on page 254.
4. When you have completed the required edits, select *OK* to close the edit element dialog box.
5. Select the *Save* icon to save your changes.

To delete a report template element:

1. Go to the *Reports* tab and select the template from the tree menu that contains to the element you would like to delete.
2. Select the delete icon in the top right corner of the element.

Figure 210: Delete an element



3. Select *OK* in the confirmation dialog box to delete the element.
4. Select the *Save* icon to save your changes.

Import and export report templates

Report templates can be imported from and exported to the management computer.

To import a report template:

1. Go to the *Reports* tab and right-click on a template in the tree menu.
2. Select *Import* in the pop-up menu.

   The *Import Report Template* dialog box opens.
3. Select *Browse* and browse to the location of the template file.
4. Select *OK* to import the report template.

To export a report template:

1. Go to the *Reports* tab and right-click on a template in the tree menu.
2. Select *Export* in the pop-up menu.
3. Select a location to save the template, then select *OK* to export the report template.

Schedules

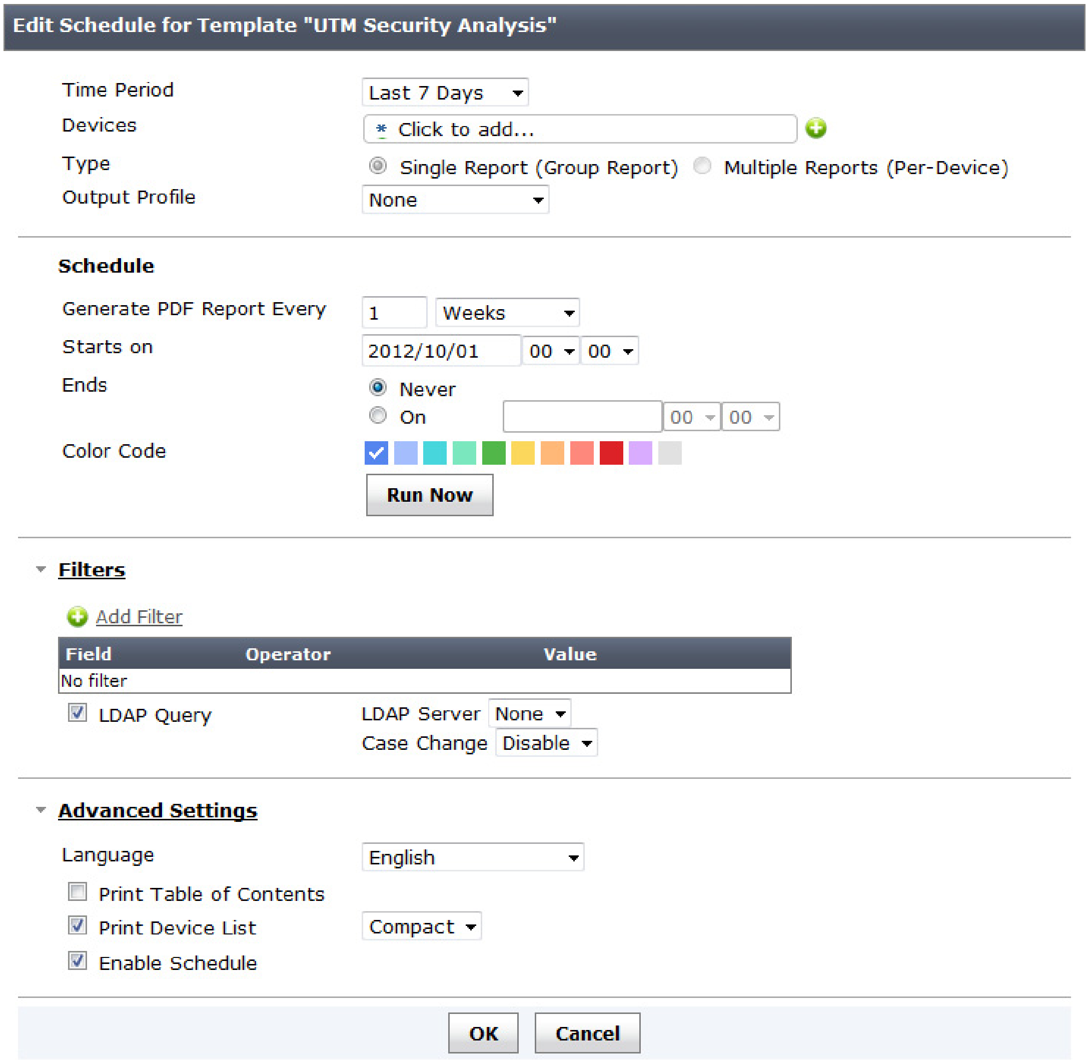
Report schedules provide a way to generate reports at specific times. You can also manually run a report schedule at any time and enable or disable report schedules.

To create a new schedule:

1. Go to the *Reports* tab and do one of the following:
   - Right-click the report template for which you would like to create a schedule in the tree menu. In the right-click menu, under the *Folder* heading, select *Schedule*.
   - Select the template for which you would like to create a schedule, and then select *Schedule* in the template toolbar.
2. If no schedule exists for that template, a dialog box will open asking if you would like to create a schedule. Select *OK* to open the schedule configuration dialog box.

   If a schedule has already been created for that template, the schedule configuration dialog box opens.

Figure 211: Schedule a report template



Edit Schedule for Template "UTM Security Analysis"

Time Period: Last 7 Days
Devices: Click to add...
Type: ○ Single Report (Group Report) ○ Multiple Reports (Per-Device)
Output Profile: None

Schedule

Generate PDF Report Every: 1 Weeks
Starts on: 2012/10/01 00 00
Ends: ● Never ○ On 00 00
Color Code: ✓ 🟦 🟦 🟦 🟩 🟩 🟨 🟧 🟥 🟥 🟪 ⬜

Filters

Field	Operator	Value
No filter		

☑ LDAP Query — LDAP Server: None; Case Change: Disable

Advanced Settings

Language: English
□ Print Table of Contents
☑ Print Device List: Compact
☑ Enable Schedule

3. Configure the following settings:

Time Period	Select the time period that the report covers from the drop-down list.
Devices	Select the specific devices or arrays that the report will cover.
Type	Select *Per Device Reports* or *Group Reports*.
Output Profile	Select an output profile for the report (optional). See “Output profiles” on page 270 for more information.
Schedule	
Generate PDF Report Every	Select when the report is generated: • Enter a number for the frequency of the report based on the time period selected from the drop-down list, or select *On Demand* to only run the report manually. • If *On Demand* is not selected, enter a starting and ending date and time for the file generation, or set it for never ending.

Starts On	Enter a starting date and time for the file generation.
Ends	Enter an ending date and time for the file generation, or set it for never ending.
Color Code	Select the color for the report schedule that will be visible on the report calendar.
Run Now	Select to run the report against the selected devices.
Filter	
Add Filter	Add a filter to the schedule.
LDAP Query	Select to enable LDAP query for the schedule. Select the LDAP Server and Case Change from the drop-down lists.
Advanced Settings	
Language	Select the report language from the drop-down menu. The default language is English.
Print Table of Contents	Select the check-box to include a table of contents in the report.
Print Device List	Select the check-box to include a device list in the report. Three styles are available from the drop-down list: • *Compact*: Display a compact comma-separated list of device names. • *Count*: Display only the number of devices. • *Detailed*: Display a table of device information for each device.
Enable Schedule	Select the check-box to enable the report schedule.

4. Select *OK* to create the report schedule.

To edit a report schedule:

1. Go to the *Reports* tab and either:
   a. right-click the report template whose schedule you would like to edit, then, under the *Folder* heading, select *Schedule*, or
   b. select *Report Calendar* in the tree menu and then select the report schedule you would like to edit from the calendar.

   The schedule configuration dialog box opens, see Figure 211 on page 260.
2. Edit the report schedule as required and select *OK* to apply the changes.

To delete a report schedule:

1. Go to the *Reports* tab and select *Report Calendar* in the tree menu.
2. Right-click the schedule you would like to delete and then select *Delete* from the pop-up menu.
3. Select OK in the confirmation dialog box to delete the report schedule.

To manually run a report schedule:

1. Go to the *Reports* tab and right-click on the report template whose schedule you would like to run.
2. In the right-click menu, under the *Template* heading, select *Schedule*.

   The schedule configuration dialog box opens.
3. Select *Run Now* to run the report schedule.

   The report schedule will run and the report will be generated. See "History" on page 262 for information on viewing the report.

To enable/disable a report schedule:

1. Go to the *Reports* tab and right-click on the report template whose schedule you would like to enable or disable.
2. In the right-click menu, under the *Template* heading, select *Schedule*.

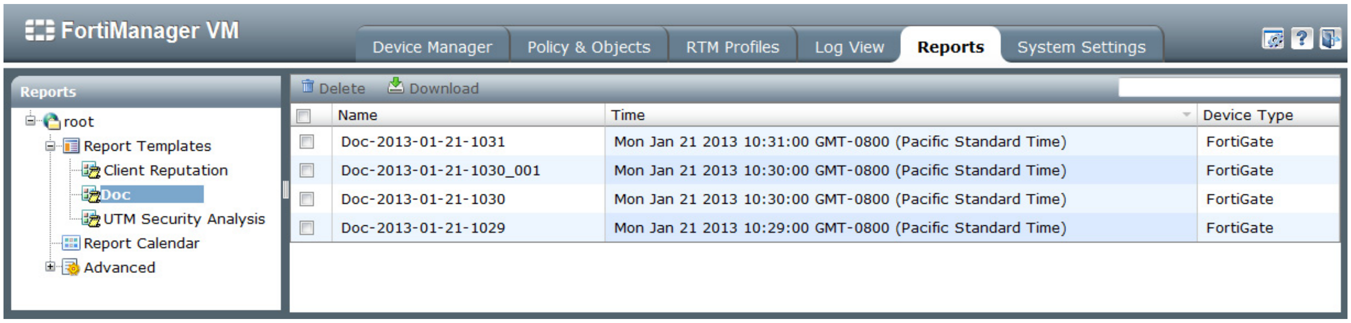
   The schedule configuration dialog box opens, see Figure 211 on page 260.
3. In the *Advanced Settings* section, check or uncheck the Enable check-box to enable or disable the report schedule.
4. Select *OK* to apply the changes.

History

Report history allows you to view all reports that have been generated for either a report template or a specific device on the FortiManager system. It displays the report name, device type, and the time that the report was generated. Select a report from the list to view the report in a new window or tab in your web-browser.

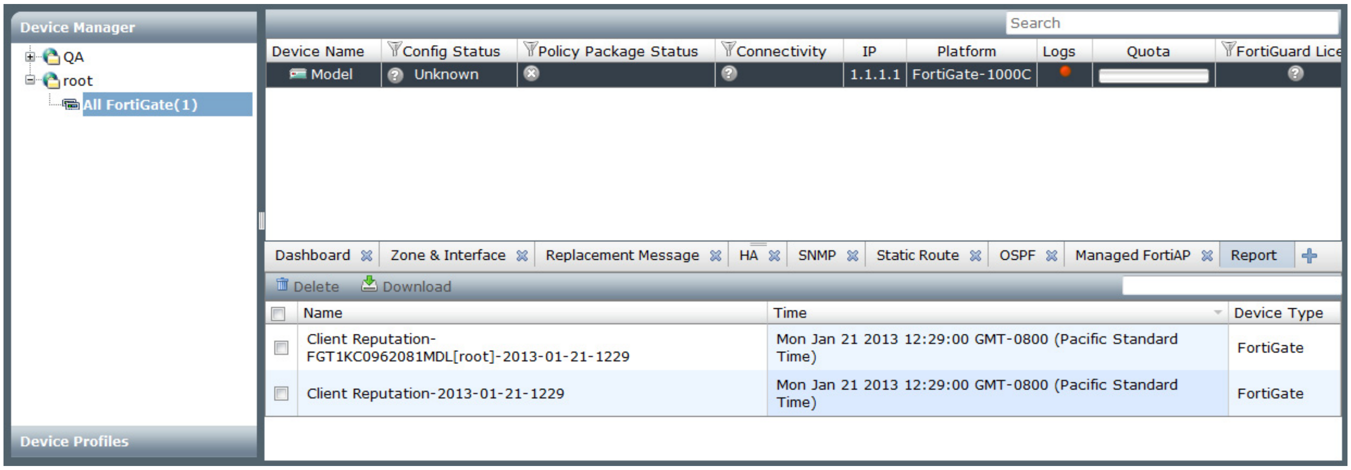
The reports can also be downloaded as PDFs, and deleted.

Figure 212: Report template history page



□	Name	Time	Device Type
□	Doc-2013-01-21-1031	Mon Jan 21 2013 10:31:00 GMT-0800 (Pacific Standard Time)	FortiGate
□	Doc-2013-01-21-1030_001	Mon Jan 21 2013 10:30:00 GMT-0800 (Pacific Standard Time)	FortiGate
□	Doc-2013-01-21-1030	Mon Jan 21 2013 10:30:00 GMT-0800 (Pacific Standard Time)	FortiGate
□	Doc-2013-01-21-1029	Mon Jan 21 2013 10:29:00 GMT-0800 (Pacific Standard Time)	FortiGate

Figure 213: Device report history page



Device Name	Config Status	Policy Package Status	Connectivity	IP	Platform	Logs	Quota	FortiGuard Lice
Model	Unknown			1.1.1.1	FortiGate-1000C	●		

☐	Name	Time	Device Type
☐	Client Reputation-FGT1KC0962081MDL[root]-2013-01-21-1229	Mon Jan 21 2013 12:29:00 GMT-0800 (Pacific Standard Time)	FortiGate
☐	Client Reputation-2013-01-21-1229	Mon Jan 21 2013 12:29:00 GMT-0800 (Pacific Standard Time)	FortiGate

To view a report history:

Historical reports can be viewed for a specific report template from the *Reports* tab or for a specific device from the *Device Manager* tab.

To view historical reports from the *Reports* tab:

1. Go to the *Reports* tab and right-click on the report template whose history you would like to view.
2. In the right-click menu, under the *Template* heading, select *Historical Reports*. This option will only be available if the report template has already been run.

   The report history page opens, see Figure 212 on page 262, showing a list of all the reports that have been run for that template.

To view historical reports from the *Device Manager* tab:

3. Go to the *Device Manager* tab and select the ADOM or device group that contains the device whose historical report you would like to view.
4. In the lower content pane, select the *Reports* tab.

   The report history is shown in the lower content pane, see Figure 213 on page 263, showing a list of all the reports that have been run for that template.

To delete reports:

1. In the report history list, select the report or reports that you would like to delete, or right-click and select *Select All* if you are deleting all of the reports.
2. Select *Delete* in the toolbar, or right-click and select *Delete* from the pop-up menu.
3. Select *OK* in the confirmation dialog box to delete the report or reports.

To download reports:

1. In the report history list, select the report or reports that you would like to download, or right-click and select *Select All* if you are downloading all of the reports.
2. Select *Download* in the toolbar, or right-click and select *Download* from the pop-up menu.
3. Save the file to your computer, or open the file in an applicable program.

   If you are downloading multiple reports, each one will be saved as a separate file.

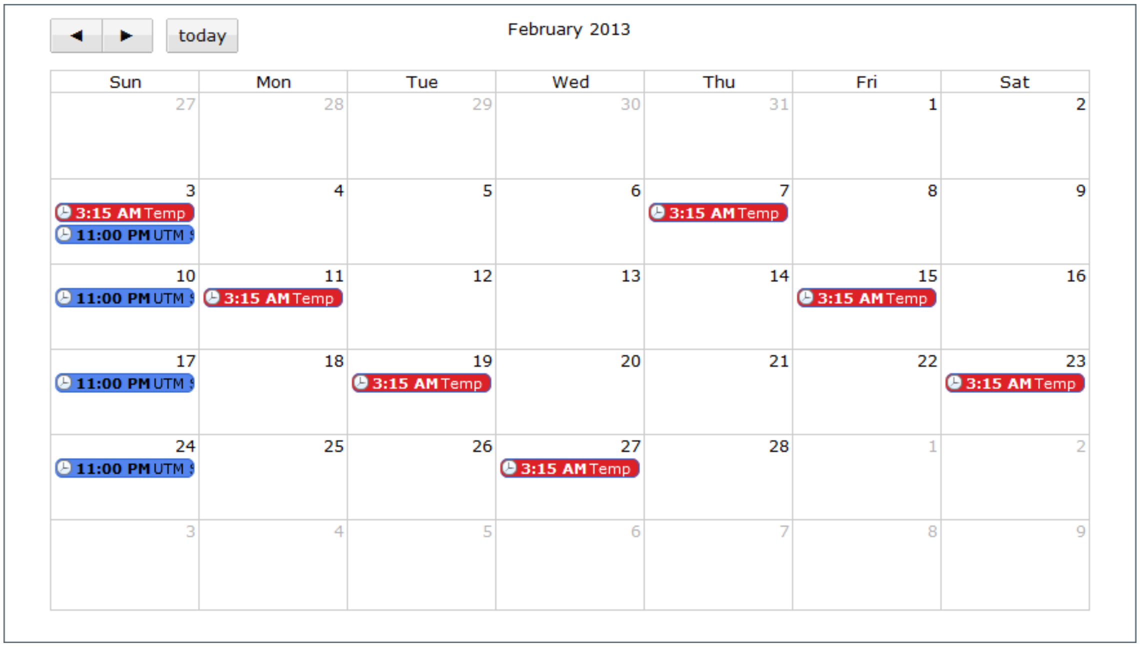
Calendar

The report calendar provides an overview of the report schedules. You can view all reports scheduled for the selected month.

Selecting a report schedule in the calendar opens the schedule configuration dialog box, allowing you to make changes to the settings for that schedule (see "Schedules" on page 259). If the report has already been run, selecting the report schedule will allow you to download the report.

To view the report calendar, go to the *Reports* tab and select *Report Calendar* in the tree menu.

Figure 214: Report calendar

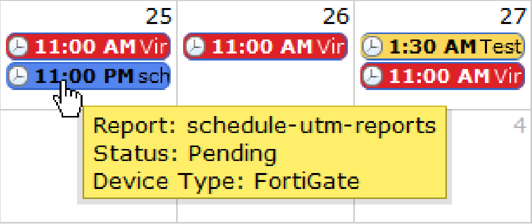


February 2013

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	31	1	2
3 3:15 AM Temp 11:00 PM UTM	4	5	6	7 3:15 AM Temp	8	9
10 11:00 PM UTM	11 3:15 AM Temp	12	13	14	15 3:15 AM Temp	16
17 11:00 PM UTM	18	19 3:15 AM Temp	20	21	22	23 3:15 AM Temp
24 11:00 PM UTM	25	26	27 3:15 AM Temp	28	1	2
3	4	5	6	7	8	9

When hovering the mouse cursor over a scheduled report on the calendar, a notification box will appear detailing the report name, status, and the device type.

Figure 215: Report schedule calendar details



25	26	27
11:00 AM Vir 11:00 PM sch	11:00 AM Vir	1:30 AM Test 11:00 AM Vir
		4

Report: schedule-utm-reports
Status: Pending
Device Type: FortiGate

Advanced

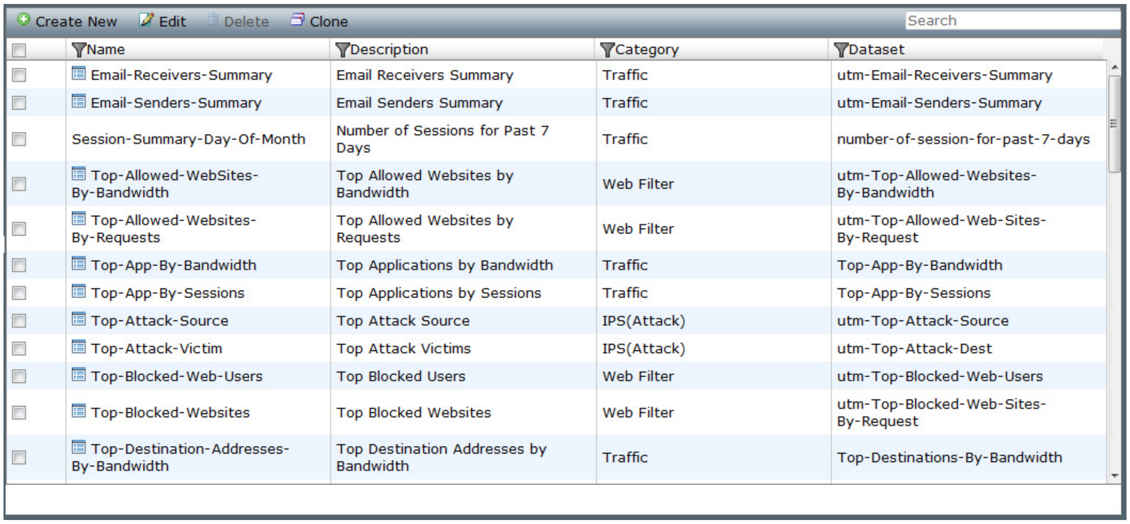
The advanced report options includes chart and dataset settings, output profiles, and report language settings.

Charts

The FortiManager unit provides a selection pre-defined charts. New charts can also be created, either from scratch or by cloning a previous chart.

To view and configure charts, go to the *Reports* tab and select *Advanced* > *Charts* in the tree menu.

Figure 216: Charts



☐	Name	Description	Category	Dataset
☐	Email-Receivers-Summary	Email Receivers Summary	Traffic	utm-Email-Receivers-Summary
☐	Email-Senders-Summary	Email Senders Summary	Traffic	utm-Email-Senders-Summary
☐	Session-Summary-Day-Of-Month	Number of Sessions for Past 7 Days	Traffic	number-of-session-for-past-7-days
☐	Top-Allowed-WebSites-By-Bandwidth	Top Allowed Websites by Bandwidth	Web Filter	utm-Top-Allowed-Websites-By-Bandwidth
☐	Top-Allowed-Websites-By-Requests	Top Allowed Websites by Requests	Web Filter	utm-Top-Allowed-Web-Sites-By-Request
☐	Top-App-By-Bandwidth	Top Applications by Bandwidth	Traffic	Top-App-By-Bandwidth
☐	Top-App-By-Sessions	Top Applications by Sessions	Traffic	Top-App-By-Sessions
☐	Top-Attack-Source	Top Attack Source	IPS(Attack)	utm-Top-Attack-Source
☐	Top-Attack-Victim	Top Attack Victims	IPS(Attack)	utm-Top-Attack-Dest
☐	Top-Blocked-Web-Users	Top Blocked Users	Web Filter	utm-Top-Blocked-Web-Users
☐	Top-Blocked-Websites	Top Blocked Websites	Web Filter	utm-Top-Blocked-Web-Sites-By-Request
☐	Top-Destination-Addresses-By-Bandwidth	Top Destination Addresses by Bandwidth	Traffic	Top-Destinations-By-Bandwidth

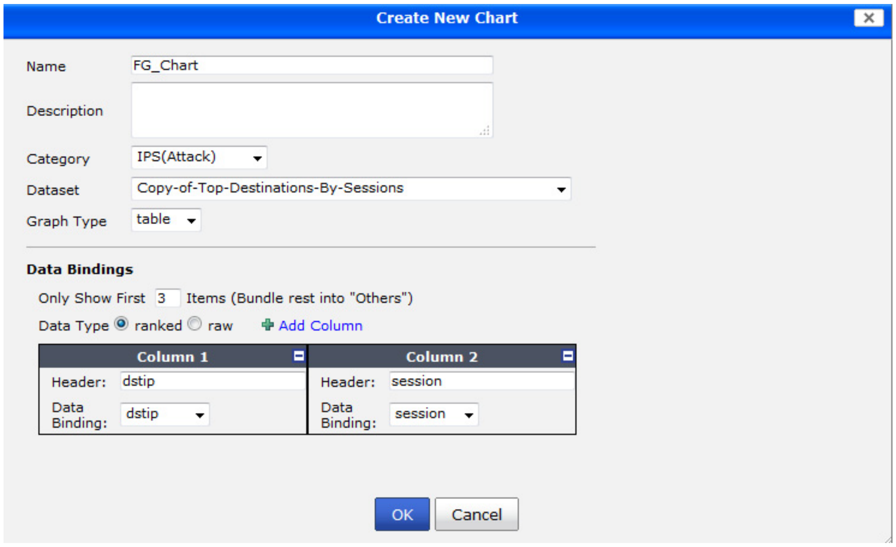
For a list of the currently available pre-defined charts, see “Charts” on page 232.

To create a new chart:

1. Go to the *Reports* tab and select *Advanced* > *Chart* in the tree menu.
2. Select *Create New* on the toolbar, or right-click in the chart list and select *New* from the pop-up menu.

   The *Create New Chart* dialog box opens.

Figure 217: Create a new chart



Create New Chart

Name: FG_Chart

Description:

Category: IPS(Attack)

Dataset: Copy-of-Top-Destinations-By-Sessions

Graph Type: table

Data Bindings

Only Show First 3 Items (Bundle rest into "Others")

Data Type ● ranked ○ raw

Column 1	Column 2
Header: dstip	Header: session
Data Binding: dstip	Data Binding: session

3. Enter the required information for the new chart.

Name	Enter a name for the chart.
Description	Enter a description.
Category	Select a category for the chart from the drop-down menu. Select one of the following: IPS(Attack), Event, Traffic, Web Filter, Virus, or Network Scan.
Dataset	Select a dataset from the drop-down list. See “Datasets” on page 267 for more information.
Graph Type	Select a graph type from the drop-down list. Select one of the following: bar, pie, table, or line.
bar, pie, or line	
Line Subtype	Select one of the following: *basic*, *stacked*, or *back-to-back*. This option is only available when *line* is selected as the graph type.
X-Axis	*Data Binding*: Select a value from the drop-down menu. *Only Show First*: Enter a numerical value. Only the first ‘X’ items will be displayed. Other items are bundled into Others. *Overwrite label*: Enter a label.
Y-Axis	*Order By*: Select a value from the drop-down menu. *Data Binding*: Select a value from the drop-down menu. *Overwrite label*: Enter a label.
table	
Only Show First Items	Enter a numerical value. Only the first ‘X’ items will be displayed. Other items are bundled into *Others*.
Data Type	Select either *ranked* or *raw*.

Columns	Up to three columns can be included. *Header*: Enter header information. *Data Binding*: Select a value from the drop-down menu.
Add Column	Select to add a column.

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

To clone a chart:

1. Go to the *Reports* tab and select *Advanced* > *Chart* in the tree menu.
2. Select the chart that you would like to clone and select *Clone* from the toolbar or right-click menu. The *Clone Chart* dialog box opens.
3. Edit the information as needed and select *OK* to clone the chart and create a new chart.

To edit a chart:

1. Go to the *Reports* tab and select *Advanced* > *Chart* in the tree menu.
2. Double-click on the chart that you would like to edit, or select the chart and select *Edit* from the toolbar or right-click menu. The *Edit Chart* dialog box opens.
3. Edit the information as required and select *OK* to finish editing the chart.

Pre-defined charts cannot be edited, the information can only be viewed.

To delete charts:

1. Go to the *Reports* tab and select *Advanced* > *Chart* in the tree menu.
2. Select the chart or charts that you would like to delete and select *Delete* from the toolbar or right-click menu.
3. Select *OK* in the confirmation dialog box to delete the chart or charts.

Pre-defined charts cannot be deleted, the information can only be viewed.

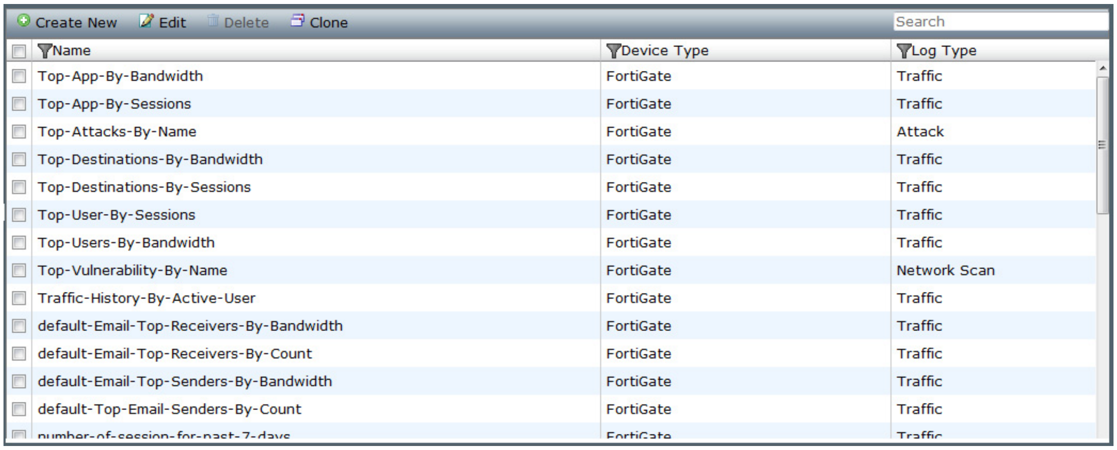
Datasets

FortiManager datasets are collections of log files from monitored devices. Reports are generated based on these datasets.

Pre-defined datasets for each supported device type are provided, and new datasets can be created and configured.

To view and configure datasets, go to the *Reports* tab and select *Advanced* > *Dataset* in the tree menu.

Figure 218: Datasets



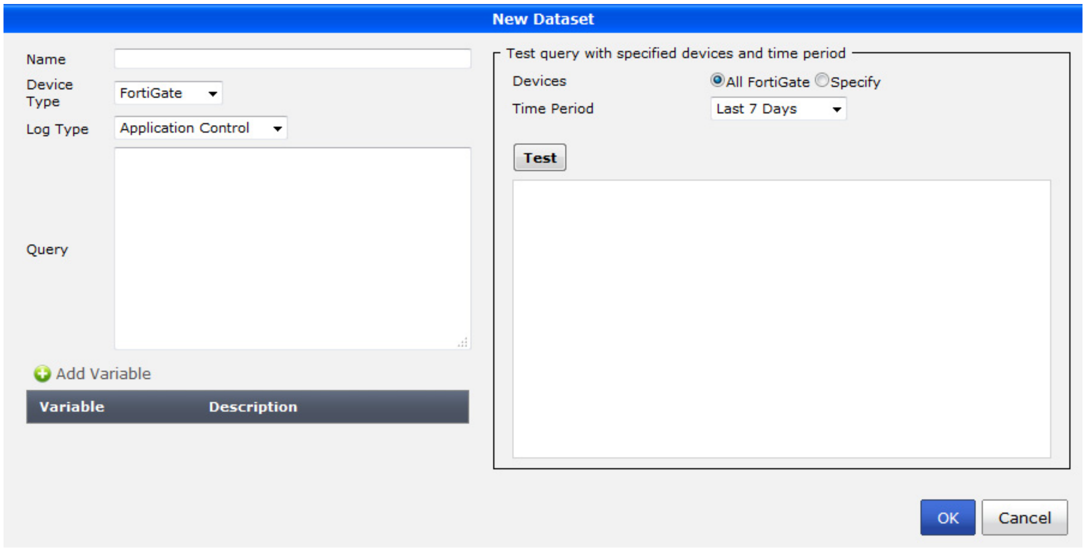
☐ Name	Device Type	Log Type
☐ Top-App-By-Bandwidth	FortiGate	Traffic
☐ Top-App-By-Sessions	FortiGate	Traffic
☐ Top-Attacks-By-Name	FortiGate	Attack
☐ Top-Destinations-By-Bandwidth	FortiGate	Traffic
☐ Top-Destinations-By-Sessions	FortiGate	Traffic
☐ Top-User-By-Sessions	FortiGate	Traffic
☐ Top-Users-By-Bandwidth	FortiGate	Traffic
☐ Top-Vulnerability-By-Name	FortiGate	Network Scan
☐ Traffic-History-By-Active-User	FortiGate	Traffic
☐ default-Email-Top-Receivers-By-Bandwidth	FortiGate	Traffic
☐ default-Email-Top-Receivers-By-Count	FortiGate	Traffic
☐ default-Email-Top-Senders-By-Bandwidth	FortiGate	Traffic
☐ default-Top-Email-Senders-By-Count	FortiGate	Traffic
☐ number-of-session-for-past-7-days	FortiGate	Traffic

To create a new dataset:

1. Go to the *Reports* tab and select *Advanced* > *Dataset* in the tree menu.
2. Select *Create New* on the toolbar, or right-click in the dataset list and select *New* from the pop-up menu.

   The *Create New* Dataset dialog box opens.

   Figure 219: Create a new dataset



Name

Device Type: FortiGate

Log Type: Application Control

Devices: ● All FortiGate ○ Specify

Time Period: Last 7 Days

3. Enter the required information for the new dataset.

Name	Enter a name for the dataset.
Device Type	Select a device type from the drop-down list. The following device types are available: FortiGate, LocalLogs, FortiClient, FortiMail, and FortiWeb.
Log Type	Select a log type from the drop-down list. The following log types are available: Application Control, Attack, DLP Archive, DLP, EmailFilter, Event, History, Network Analyzer, Traffic, Virus, WebFilter, and Network Scan.

SQL Query	Enter the SQL query used for the dataset.
Add Variable	Select to add a variable and description information.
Test query with specified devices and time period	Select devices and test the SQL query against the new dataset. In FortiManager v5.0 Patch Release 2 or later you can test the query against specific devices or a log array.
Devices	Select *All FortiGates* or *Specify* to select specific devices or log arrays to run the SQL query against.
Time Period	Use the drop-down menu to select a time period.
Test	Select to test the SQL query before saving the dataset configuration.

4. When you are satisfied that the SQL query functions as expected, select *OK* to create the new dataset.

To clone a dataset:

1. Go to the *Reports* tab and select *Advanced* > *Dataset* in the tree menu.
2. Select the dataset that you would like to clone and select *Clone* from the toolbar or right-click menu. The *Clone Dataset* dialog box opens.
3. Edit the information as needed and select *OK* to clone the dataset and create a new dataset.

To edit a dataset:

1. Go to the *Reports* tab and select *Advanced* > *Dataset* in the tree menu.
2. Double-click on the dataset that you would like to edit, or select the dataset and select *Edit* from the toolbar or right-click menu. The *Edit Dataset* dialog box opens.

Pre-defined datasets cannot be edited, the information is read-only. You can view the SQL query and variables used in the dataset and test against specific devices or log arrays.

3. Edit the information as required and select *OK* to finish editing the dataset.

To delete datasets:

1. Go to the *Reports* tab and select *Advanced* > *Dataset* in the tree menu.
2. Select the dataset or datasets that you would like to delete and select *Delete* from the toolbar or right-click menu.

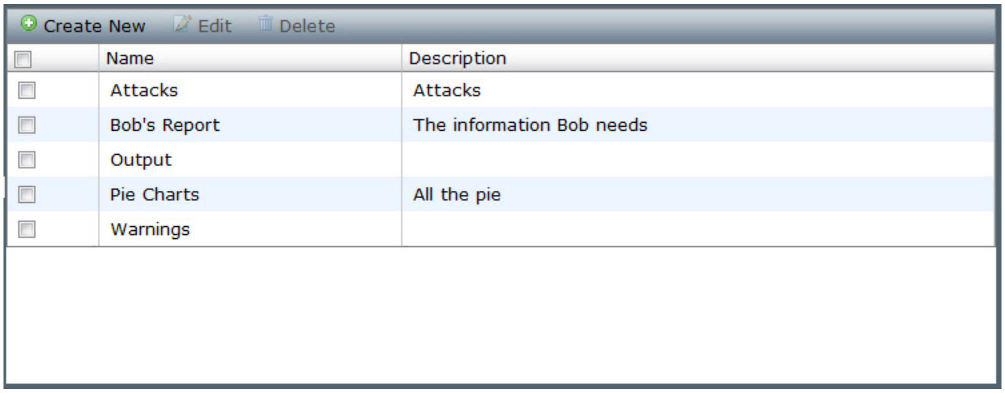
Pre-defined datasets cannot be deleted, the information is read-only.

3. Select *OK* in the confirmation dialog box to delete the datasets or datasets.

Output profiles

Output profiles allow you to define email addresses to which generated reports are sent, and provides an option to upload the reports to FTP, SFTP, or SCP servers. Once created, an output profile can be specified in a report schedule; see “Schedules” on page 259.

Figure 220: Output profile page



□	Name	Description
□	Attacks	Attacks
□	Bob's Report	The information Bob needs
□	Output	
□	Pie Charts	All the pie
□	Warnings	

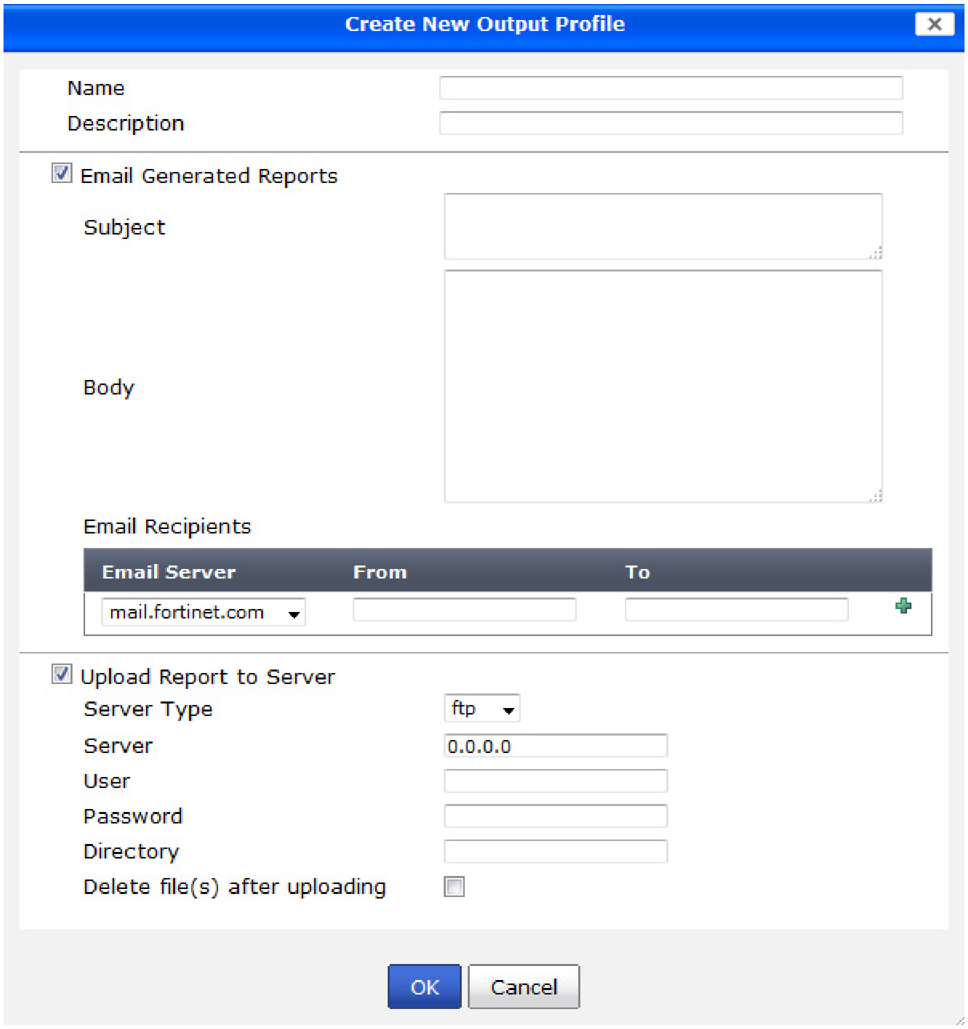
You must configure a mail server before you can configure an output profile. Please see “Mail server” on page 107 for information on configuring a mail server.

To create a new output profile:

1. Go to the *Reports* tab and select *Advanced* > *Output Profile* in the tree menu.
2. Select *Create New* on the toolbar, or right-click in the output profile list and select *New* from the pop-up menu.

   The *Create New Output Profile* dialog box opens.

Figure 221: Create new output profile dialog box



Create New Output Profile

Name

Description

☑ Email Generated Reports

Subject

Body

Email Recipients

Email Server	From	To
mail.fortinet.com		

☑ Upload Report to Server

Server Type: ftp

Server: 0.0.0.0

User

Password

Directory

Delete file(s) after uploading □

3. Enter the following information:

Name	Enter a name for the new output profile.
Description	Enter a description for the output profile (optional).
Email Generated Reports	Enable email generated reports.
Subject	Enter a subject for the report email.
Body	Enter body text for the report email.
Email Recipients	Select the email server from the drop-down list and enter to and from email addresses. Select the + icon to add another entry so that you can specify multiple recipients.
Upload Report to Server	Enable uploading the reports to a server.
Server Type	Select FTP, SFTP, or SCP from the drop-down list.
Server	Enter the server IP address.

User	Enter the username.
Password	Enter the password.
Directory	Specify the directory where the report will be saved.
Delete file(s) after uploading	Select to delete the report after it has been uploaded to the selected.

4. Select OK to create the new output profile.

To edit an output profile:

1. Go to the *Reports* tab and select *Advanced* > *Output Profile* in the tree menu.
2. Double-click on the output profile that you would like to edit, or select the output profile and select *Edit* from the toolbar or right-click menu. The *Edit Output Profile* dialog box opens.
3. Edit the information as required and select *OK* to finish editing the output profile.

To delete output profiles:

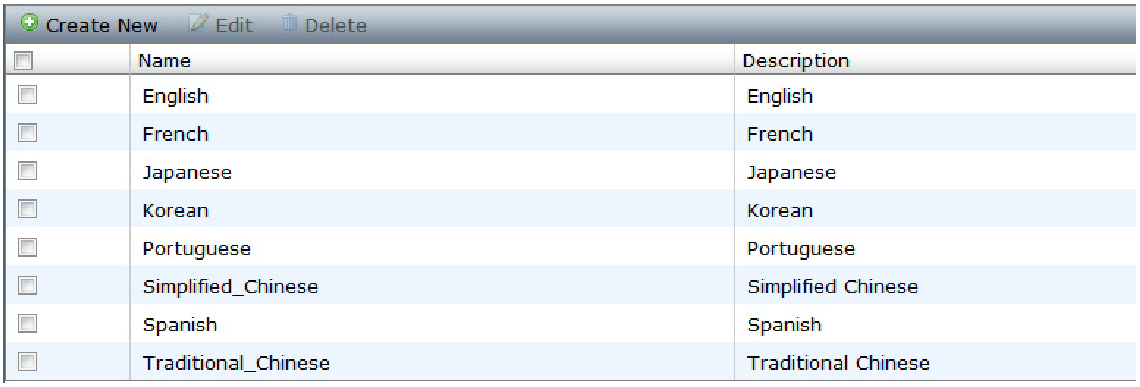
1. Go to the *Reports* tab and select *Advanced* > *Output Profile* in the tree menu.
2. Select the output profile or profiles that you would like to delete and select *Delete* from the toolbar or right-click menu.
3. Select *OK* in the confirmation dialog box to delete the selected output profile or profiles.

Language

The language of the reports can be specified when creating a report schedule (see "Schedules" on page 259). New languages can be added, and the name and description of the languages can be changed. The pre-defined languages cannot be edited.

The available report languages can be viewed in the *Reports* tab under *Advanced* > *Language*.

Figure 222: Report language



□	Name	Description
□	English	English
□	French	French
□	Japanese	Japanese
□	Korean	Korean
□	Portuguese	Portuguese
□	Simplified_Chinese	Simplified Chinese
□	Spanish	Spanish
□	Traditional_Chinese	Traditional Chinese

The available preconfigured report languages include:

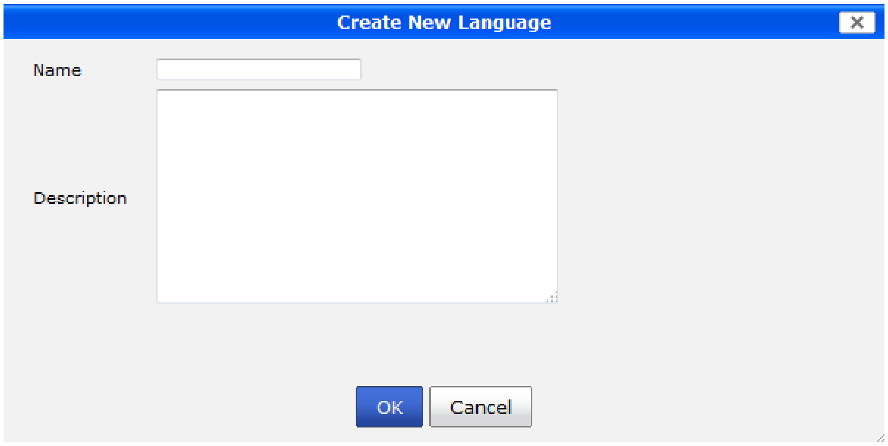
- English (default report language)
- French
- Japanese
- Korean
- Portuguese
- Simplified Chinese
- Spanish
- Traditional Chinese

To add a language:

1. Go to the *Reports* tab and select *Advanced* > *Language* in the tree menu.
2. Select *Create New* on the toolbar, or right-click in the language list and select *New* from the pop-up menu.

   The *Create New Language* dialog box opens.

   Figure 223: Create a new language

3. Enter a name and description for the language in the requisite fields.
4. Select *OK* to add the language.

Adding a new language does not create that language. It only adds a placeholder for that language that contains the language name and description.

To edit a language:

1. Go to the *Reports* tab and select *Advanced* > *Language* in the tree menu.
2. Double-click on the language that you would like to edit, or select the language and select *Edit* from the toolbar or right-click menu. The *Edit Language* dialog box opens.

3. Edit the information as required and select *OK* to finish editing the language.

Pre-defined languages cannot be edited. The information can only be viewed.

To delete languages:

1. Go to the *Reports* tab and select *Advanced* > *Language* in the tree menu.
2. Select the language or languages that you would like to delete and select *Delete* from the toolbar or right-click menu.
3. Select *OK* in the confirmation dialog box to delete the selected language or languages.

Pre-defined languages cannot be deleted.

FortiGuard Center

The FortiGuard Distribution Network (FDN) provides FortiGuard services for your FortiManager system and its managed devices and FortiClient agents. The FDN is a world-wide network of FortiGuard Distribution Servers (FDS) which update the FortiGuard services on your FortiManager system on a regular basis so that your FortiManager system is protected against the latest threats.

The FortiGuard services available on the FortiManager system include:

- Antivirus and IPS engines and signatures
- Web filtering and email filtering rating databases and lookups (select systems)

To view and configure these services, go to *FortiGuard* > *Advanced Settings*.

In FortiGuard Center, you can configure the FortiManager system to act as a local FDS, or use a web proxy server to connect to the FDN. FortiManager systems acting as a local FDS synchronize their FortiGuard service update packages with the FDN, then provide FortiGuard these updates and look up replies to your private network's FortiGate devices. The local FDS provides a faster connection, reducing Internet connection load and the time required to apply frequent updates, such as antivirus signatures, to many devices.

As an example, you might enable FortiGuard services to FortiGate devices on the built-in FDS, then specify the FortiManager system's IP address as the override server on your devices. Instead of burdening your Internet connection with all the devices downloading antivirus updates separately, the FortiManager system would use the Internet connection once to download the FortiGate antivirus package update, then redistribute the package to the devices.

FortiGuard Center also includes firmware revision management. To view and configure firmware options, go to *FortiGuard* > *Firmware Images*. You can download these images from the Customer Service & Support site to install on your managed devices or on the FortiManager system.

Before you can use your FortiManager system as a local FDS, you must:

- Register your devices with Fortinet Customer Service & Support and enable the FortiGuard service licenses. See your device documentation for more information on registering your products.
- If the FortiManager system's Unregistered Device Options do not allow service to unregistered devices, add your devices to the device list, or change the option to allow service to unregistered devices.

  For information about FDN service connection attempt handling or adding devices, see "Device Manager" on page 114.
- Enable and configure the FortiManager system's built-in FDS. For more information, see "Configuring network interfaces" on page 71.
- Connect the FortiManager system to the FDN.

  The FortiManager system must retrieve service update packages from the FDN before it can redistribute them to devices and FortiClient agents on the device list. For more information, see "Connecting the built-in FDS to the FDN" on page 283.
- Configure each device or FortiClient endpoint to use the FortiManager system's built-in FDS as their override server. You can do this when adding a FortiGate system. For more information, see "Adding a device" on page 130.

This section contains the following topics:

- Advanced settings
- Configuring devices to use the built-in FDS
- Configuring FortiGuard services
- Logging events related to FortiGuard services
- Restoring the URL or antispam database
- Package management
- Query server management
- Firmware images

For information on current security threats, virus and spam sample submission, and FortiGuard service updates available through the FDN, including antivirus, IPS, web filtering, and email filtering, see the FortiGuard web site, http://www.fortiguard.com/.

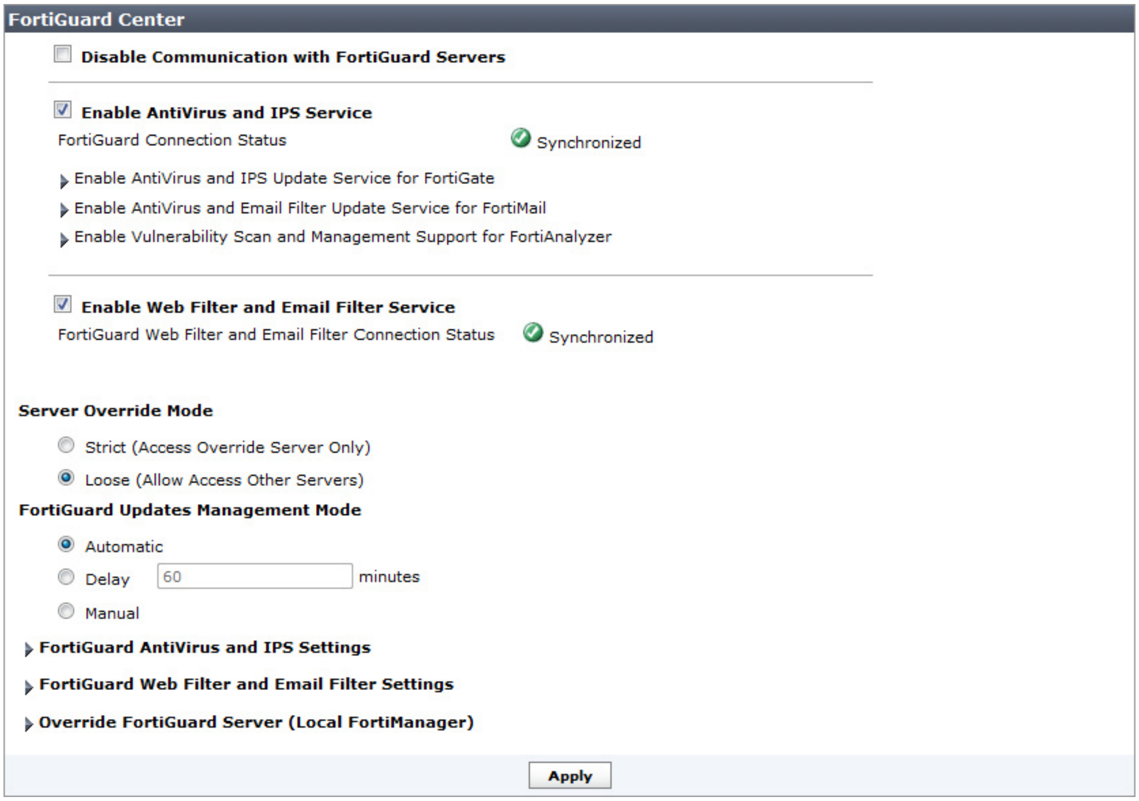
Advanced settings

The advanced settingsprovides 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 configuring your devices to use the FortiManager system as their FortiGuard server, you can view overall and per device statistics on FortiGuard service benefits. The FortiGuard Center has three supported configuration options:

- Antivirus and IPS Update Service for FortiGate
- Antivirus and email filter update Service for FortiMail
- Vulnerability Scan and Management Support for FortiAnalyzer

Figure 224: FortiGuard advanced settings



FortiGuard Center

□ Disable Communication with FortiGuard Servers

☑ Enable AntiVirus and IPS Service

FortiGuard Connection Status ✓ Synchronized

▸ Enable AntiVirus and IPS Update Service for FortiGate
▸ Enable AntiVirus and Email Filter Update Service for FortiMail
▸ Enable Vulnerability Scan and Management Support for FortiAnalyzer

☑ Enable Web Filter and Email Filter Service

FortiGuard Web Filter and Email Filter Connection Status ✓ Synchronized

Server Override Mode

○ Strict (Access Override Server Only)
● Loose (Allow Access Other Servers)

FortiGuard Updates Management Mode

● Automatic
○ Delay 60 minutes
○ Manual

▸ FortiGuard AntiVirus and IPS Settings
▸ FortiGuard Web Filter and Email Filter Settings
▸ Override FortiGuard Server (Local FortiManager)

Disable Communication with FortiGuard Servers Disable communication with the FortiGuard servers.

Enable Antivirus and IPS Service Select to enable antivirus and intrusion protection service.

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.

Enable Antivirus and IPS Update Service for FortiGate Select the OS versions from the table for updating antivirus and intrusion protection for FortiGate.

Enable Antivirus and Email Filter Update Service for FortiMail Select the OS versions from the table for updating antivirus and email filter for FortiMail.

Enable Vulnerability Scan and Management Support for FortiAnalyzer

Select the OS versions from the table for supporting Vulnerability Scan and Management Support for FortiAnalyzer.

Enable Web Filter and Email Filter Services

Select to enable web filter and email filter services.

FortiGuard Web Filter and Email Filter 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.

Server Override Mode

Select *Strict* or *Loose* override mode.

FortiGuard Updates Management Mode

Select the FortiGuard update mode:

- *Automatic*: FortiGuard updates are done automatically.
- *Delay*: Enter the delay time, in minutes, before the updates are done.
- *Manual*: FortiGuard updates must be done manually.

FortiGuard Antivirus and IPS Settings

FortiGuard Distribution Network (FDN)

Select the required settings from the following options:

- *Use Override Service Address for FortiGate/FortiMail*
- *Allow Push Update*: enter IP address and port if selected
- *Use Web Proxy*: enter IP address, port, user name, and password is selected
- *Schedule Regular Updates*: enter the update frequency if selected.

Click *Update* to apply the changes.

Advanced

Select whether or not Update Entries from FDS Server and Update Histories for Each FortiGate are logged.

FortiGuard Web Filter and Email Filter Settings

Connection to FDS Server(s)

Select the required settings from the following options:

- *Use Override Service Address for FortiGate/FortiMail*
- *Use Web Proxy*: enter IP address, port, user name, and password is selected
- *Polling Frequency*: enter the polling frequency

Click *Update* to apply the changes.

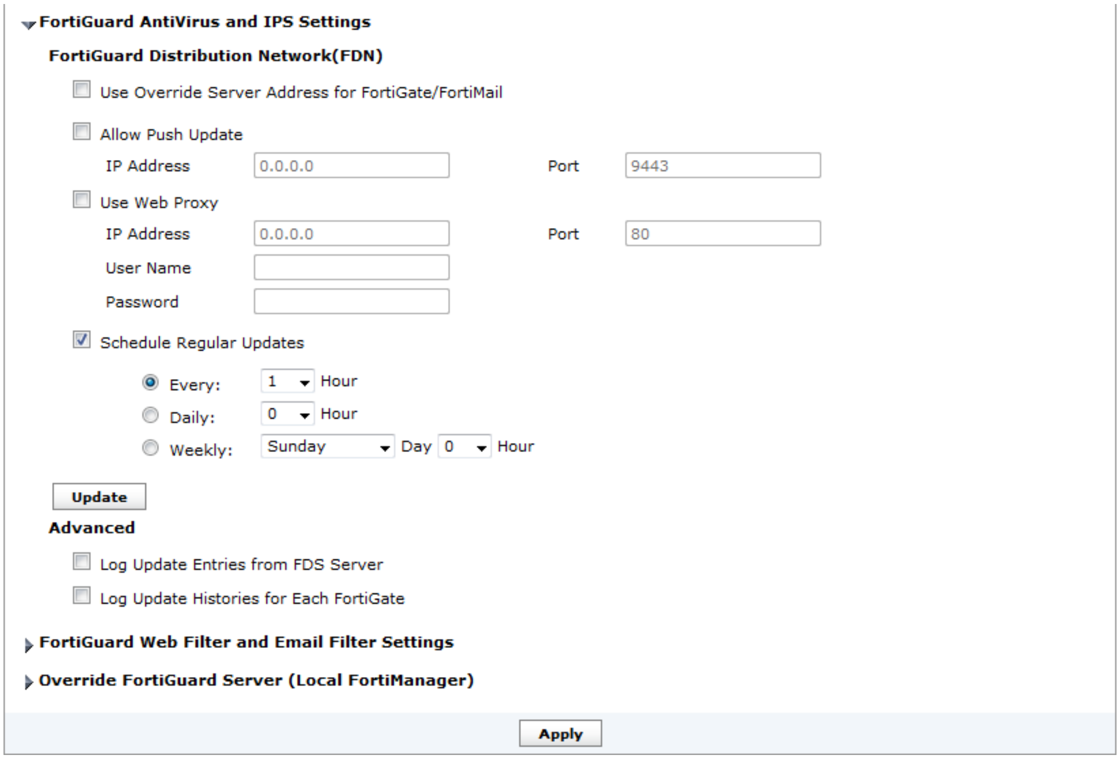
Log Settings	Select the required settings from the following options: • *Log FortiGuard Server Update Events*: enable or disable • *FortiGuard Web Filtering*: choose from *Log URL disabled*, *Log non-url events*, *Log all URL lookups* • *FortiGuard Anti-spam*: choose from *Log Spam disabled*, *Log non-spam events*, *Log all Spam lookups* • *FortiGuard Anti-virus Query*: choose from *Log Virus disabled*, *Log non-virus events*, *Log all Virus lookups*.

Override FortiGuard Server (Local FortiManager)

Additional Number of Private FortiGuard Servers	Click on the plus icon on the right side of the column to add additional private servers. Enter the IP address and selected the time zone of the private server to be added.
Enable Antivirus and IPS Update Service for Private Server	Select to enable antivirus and IPS update service for private servers.
Enable Web Filter and Email Filter Update Service for Private Server	Select to enable web filter and email filter update service for private servers.
Allow FortiGates to Access Public FortiGuard Servers when Private Servers are Unavailable	Select to allow FortiGates to access public FortiGuard servers when private serves are unavailable.

FortiGuard antivirus and IPS settings

Figure 225: FortiGuard antivirus and IPS settings



▾ FortiGuard AntiVirus and IPS Settings

FortiGuard Distribution Network(FDN)

□ Use Override Server Address for FortiGate/FortiMail

□ Allow Push Update

IP Address 0.0.0.0 Port 9443

□ Use Web Proxy

IP Address 0.0.0.0 Port 80

User Name

Password

☑ Schedule Regular Updates

● Every: 1 Hour

○ Daily: 0 Hour

○ Weekly: Sunday Day 0 Hour

Update

Advanced

□ Log Update Entries from FDS Server

□ Log Update Histories for Each FortiGate

▸ FortiGuard Web Filter and Email Filter Settings

▸ Override FortiGuard Server (Local FortiManager)

Apply

Use Override Server Address for FortiGate

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 FortiGate device’s FortiGuard services, see “Overriding default IP addresses and ports” on page 286.

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 286.

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 286.

Scheduled Regular Updates

Configure when packages are updated without manually initiating an update request.

To schedule regular service updates, see “Scheduling updates” on page 287.

Update

Select to immediately update the configured antivirus and email filter settings.

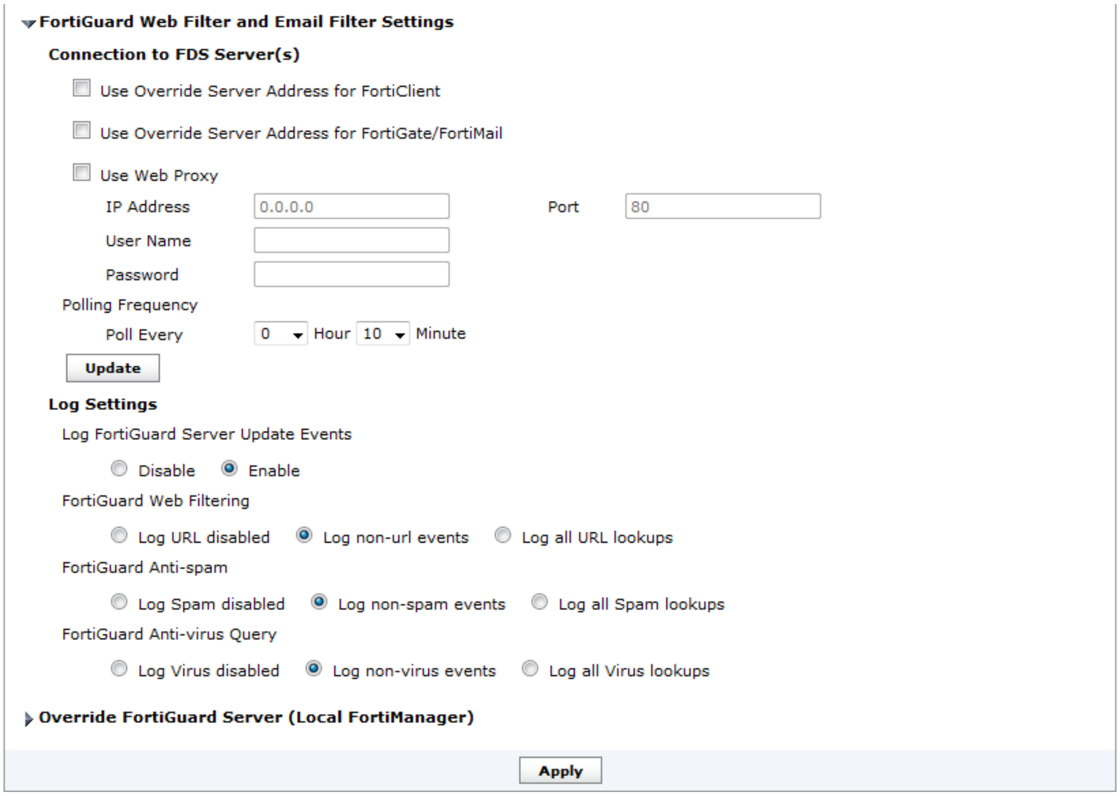
Advanced

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 and email filter settings

Figure 226: FortiGuard web filter and email filter settings



FortiGuard Web Filter and Email Filter Settings

Connection to FDS Server(s)

□ Use Override Server Address for FortiClient

□ Use Override Server Address for FortiGate/FortiMail

□ Use Web Proxy

IP Address: 0.0.0.0 Port: 80

User Name:

Password:

Polling Frequency

Poll Every: 0 Hour 10 Minute

Update

Log Settings

Log FortiGuard Server Update Events

○ Disable ● Enable

FortiGuard Web Filtering

○ Log URL disabled ● Log non-url events ○ Log all URL lookups

FortiGuard Anti-spam

○ Log Spam disabled ● Log non-spam events ○ Log all Spam lookups

FortiGuard Anti-virus Query

○ Log Virus disabled ● Log non-virus events ○ Log all Virus lookups

Override FortiGuard Server (Local FortiManager)

Apply

Connection to FDS server(s)

Configure connections for overriding the default built-in FDS or web proxy server for web filter and email filter settings.

To override an FDS server for web filter and email filter services, see “Overriding default IP addresses and ports” on page 286.

To enable web filter and email filter service updates using a web proxy server, see “Enabling updates through a web proxy” on page 286.

Log Settings

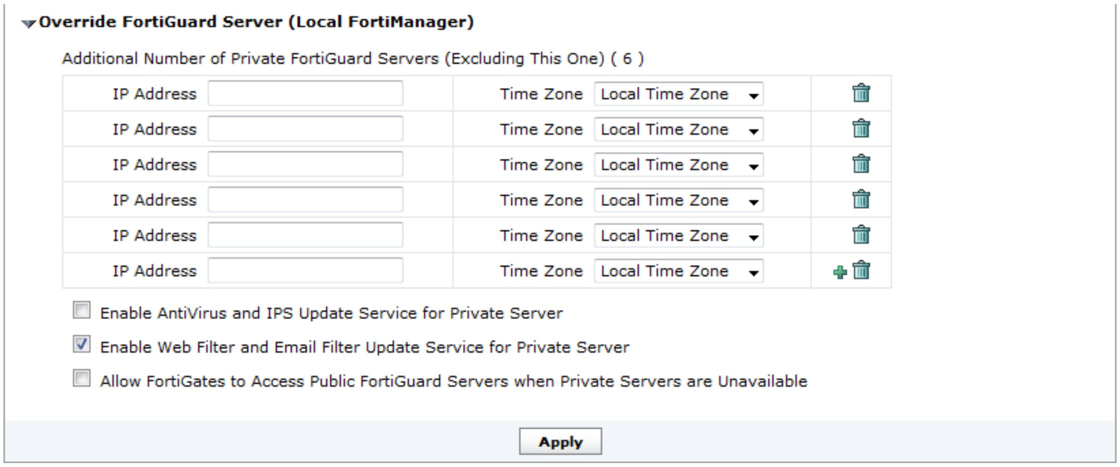
Configure logging of FortiGuard web filtering and email filter events or configure access to

To configure logging of FortiGuard web filtering and email filtering events, see “Logging FortiGuard web or email filter events” on page 289

Override FortiGuard server

Configure and enable alternate FortiManager FDS devices, rather than using the local FortiManager system. You can set up as many alternate FDS locations, and select what services are used.

Figure 227: Override FortiGuard server



Override FortiGuard Server (Local FortiManager)

Additional Number of Private FortiGuard Servers (Excluding This One) (6)

IP Address		Time Zone	Local Time Zone	
IP Address		Time Zone	Local Time Zone	
IP Address		Time Zone	Local Time Zone	
IP Address		Time Zone	Local Time Zone	
IP Address		Time Zone	Local Time Zone	
IP Address		Time Zone	Local Time Zone	+

□ Enable AntiVirus and IPS Update Service for Private Server

☑ Enable Web Filter and Email Filter Update Service for Private Server

□ Allow FortiGates to Access Public FortiGuard Servers when Private Servers are Unavailable

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.

Enable Antivirus and IPS Update Service for Private Server

When one or more private FortiGuard servers are configured, update antivirus and IPS through this private server instead of using the default FDN.

This option is available only when a private server has been configured.

Enable Web Filter and Email Filter Update Service for Private Server

When one or more private FortiGuard servers are configured, update the web filter and email filter through this private server instead of using the default FDN.

This option is available only when a private server has been configured.

Allow FortiGates to access public FortiGuard servers when private servers unavailable

When one or more private FortiGuard servers are configured, managed FortiGate units will go to those private servers for FortiGuard updates. Enable this feature to allow those FortiGate units to then try to access the public FDN servers if the private servers are unreachable.

This option is available only when a private server has been configured.

The FortiManager system’s network interface settings can restrict which network interfaces provide FDN services. For more information, see “Configuring network interfaces” on page 71.

Connecting the built-in FDS to the FDN

When you enable the built-in FDS and initiate an update either manually or by a schedule, the FortiManager system attempts to connect to the FDN.

If all connection attempts to the server list fail, the connection status will be *Disconnected*.

If the connection status remains *Disconnected*, you may need to configure the FortiManager system's connection to the FDN by:

- overriding the default IP address and/or port
- configuring a connection through a web proxy

After establishing a connection with the FDN, the built-in FDS can receive FortiGuard service update packages, such as antivirus engines and signatures or web filtering database updates, from the FDN.

To enable the built-in FDS:

1. Go to *FortiGuard* > *Advanced Settings*.
2. Enable the types of FDN services that you want to provide through your FortiManager system's built-in FDS.

   For more information, see "Configuring FortiGuard services" on page 285.
3. Select *Apply*.

   The built-in FDS attempts to connect to the FDN. To see the connection status go to *FortiGuard* > *Advanced Settings*.

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 "Configuring network interfaces" on page 71.

If you still cannot connect to the FDN, check routes, DNS, and any intermediary firewalls or NAT devices for policies that block necessary FDN ports and protocols. For additional FDN troubleshooting information, including FDN server selection, "FDN port numbers and protocols" on page 287 and the Knowledge Base article FortiGuard 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.

Procedures for configuring devices to use the built-in FDS vary by device type. See the documentation for your device for more information.

If you are connecting a device to a FortiManager system's built-in FDS, some types of updates, such as antivirus engine updates, require you to enable SSH and HTTPS Administrative Access on the network interface which will receive push updates. If the settings are disabled, see "Network" on page 69.

Matching port settings

When configuring a device to override default FDN ports and IP addresses with that of a FortiManager system, the default port settings for the device's update or query requests may not match the listening port of the FortiManager system's built-in FDS. If this is the case, the device's requests will fail. To successfully connect them, you must match the devices' port settings with the FortiManager system's built-in FDS listening ports.

For example, the default port for FortiGuard antivirus and IPS update requests is TCP 443 on FortiOS v4.0 and higher, but the FortiManager system's built-in FDS listens for those requests on TCP 8890. In this case, the FortiGate unit's update requests would fail until you configure the unit to send requests on TCP 8890.

In some cases, the device may not be configurable; instead, you must configure the FortiManager system to listen on an alternate port.

Handling connection attempts from unregistered devices

The built-in FDS replies to FortiGuard update and query connections from devices registered with the device manager's device list. If the FortiManager is configured to allow connections from unregistered devices, unregistered devices can also connect.

For example, you might choose to manage a FortiGate unit's firmware and configuration locally (from its 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 based on how it is configured. Connection attempt handling is only configurable via the CLI

To configure connection attempt handling:

1. Go to the CLI console widget in the *System Settings* tab. For information on widget settings, see "Customizing the dashboard" on page 50.
2. Click inside the console to connect.
3. Enter the following CLI command to allow unregistered devices to be registered:

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

4. To configure the system to add unregistered devices and allow service requests, enter the following CLI commands:

```
config system admin setting
  set unreg_dev_opt add_allow_service
end
```

5. To configure the system to add unregistered devices but deny service requests, enter the following CLI commands:

```
config system admin setting
  set unreg_dev_opt add_no_service
end
```

For more information, see the *FortiManager CLI Reference*.

Configuring FortiGuard services

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 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 286.

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.

The built-in FDS may not receive push updates if the external IP address of any intermediary NAT device is dynamic (such as an IP address from PPPoE or DHCP). When the NAT device's external IP address changes, the FortiManager system's push IP address configuration becomes out-of-date.

To enable push updates to the FortiManager system:

1. Go to *FortiGuard* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*; see Figure 225 on page 280.
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 *FortiGuard > Advanced Settings*.
2. If configuring a web proxy server to enable web and email filtering updates, expand *FortiGuard Web Filter and Email Filter Settings.*

   If configuring a web proxy to enable antivirus and IPS updates, expand *FortiGuard Antivirus and IPS Settings*; Figure 225 on page 280.
3. Select the check box beside *Use Web Proxy* and enter the IP address and port number of the proxy.
4. If the proxy requires authentication, enter the user name and password.
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.
6. Select *Apply*.

If the FDN connection status is *Disconnected*, the FortiManager system is unable to connect through the web proxy.

Overriding default IP addresses and ports

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 *FortiGuard > Advanced Settings*.
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*, then select the check box beside *Use Override Server Address for FortiGate/FortiMail* and enter the IP address and/or port number for all FortiGate units.

3. 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.

4. If you want to override the FortiManager system's default IP address or port for synchronizing with available FortiGuard web and email filtering updates, select the arrow to expand *FortiGuard Web Filter and Email Filter Settings*.

   Select the appropriate check box beside *Use Override Server Address for FortiGate/FortiMail* and/or *Use Override Server Address for FortiClient* and enter the IP address and/or port number.

5. Select *Apply*.

If the FDN connection status remains disconnected, the FortiManager system is unable to connect with the configured override.

FDN port numbers and protocols

Both the built-in FDS and devices use certain protocols and ports to successfully request and receive updates from the FDN or override server. Any intermediary proxies or firewalls must allow these protocols and ports, or the connection will fail.

For troubleshooting information and details on FDN ports, see and the Knowledge Base 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 283.

Scheduling updates

Keeping the built-in FDS up-to-date is important to provide current FortiGuard update packages and rating lookups to requesting devices. This is especially true as new viruses, malware, and spam sources pop up on a very frequent basis. By configuring a scheduled update, you are guaranteed to have a relatively recent version of database updates.

A FortiManager system acting as an FDS synchronizes its local copies of FortiGuard update packages with the FDN when:

- you manually initiate an update request by selecting *Update Now*
- it is scheduled to poll or update its local copies of update packages
- if push updates are enabled, it receives an update notification from the FDN

If the network is interrupted when the FortiManager system is downloading a large file, it downloads all files again when the network resumes.

To schedule antivirus and IPS updates:

1. Go to *FortiGuard* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*; Figure 225 on page 280.
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 Email Filter polling:

1. Go to *FortiGuard* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Web Filter and Email Filter Settings*.
3. In *Polling Frequency*, select the number of hours and minutes of the polling interval.

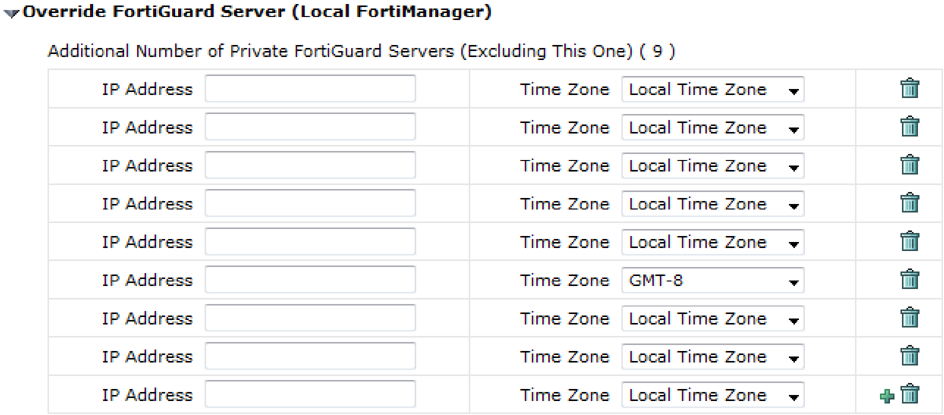
4. Select *Apply*.

If you have formatted your FortiManager system’s hard disk, polling and lookups will fail until you restore the URL and email filter databases. For more information, see “Restoring the URL or antispam database” on page 290.

Accessing public FortiGuard web and email filter servers

You can configure the FortiManager system to allow the managed FortiGate units to access public FortiGuard web filter or email filter network servers in the event local FortiGuard web filter or email filter server URL lookups fail. You can specify private servers where the FortiGate units can send URL queries.

Figure 228: Overriding FortiGuard Server



Override FortiGuard Server (Local FortiManager)

Additional Number of Private FortiGuard Servers (Excluding This One) (9)

IP Address		Time Zone	Local Time Zone	
IP Address		Time Zone	Local Time Zone	
IP Address		Time Zone	Local Time Zone	
IP Address		Time Zone	Local Time Zone	
IP Address		Time Zone	Local Time Zone	
IP Address		Time Zone	GMT-8	
IP Address		Time Zone	Local Time Zone	
IP Address		Time Zone	Local Time Zone	
IP Address		Time Zone	Local Time Zone	

To access public FortiGuard web and email filter servers:

1. Go to *FortiGuard* > *Advanced Settings*.
2. Expand *Override FortiGuard Server (Local FortiManager)*.
3. Select the *Plus* sign next to *Additional number of private FortiGuard servers (excluding this one) (0)*.
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 Email Filter 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*.

Logging events related to FortiGuard services

You can log a variety of events related to FortiGuard services.

Logging events from the FortiManager system's built-in FDS requires that you also enable local event logging.

Logging FortiGuard antivirus and IPS updates

You can track FortiGuard antivirus and IPS updates to both the FortiManager system's built-in FDS and any registered FortiGate devices which use the FortiManager system's FDS.

To log updates and histories to the built-in FDS:

1. Go to *FortiGuard* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*; see Figure 225 on page 280.
3. Under the *Advanced* heading, enable *Log Update Entries from FDS Server*.
4. Select *Apply*.

To log updates to FortiGate devices:

1. Go to *FortiGuard* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*; see Figure 225 on page 280.
3. Under the *Advanced* heading, enable *Log Update Histories for Each FortiGate*.
4. Select *Apply*.

Logging FortiGuard web or email filter events

You can track FortiGuard web filtering and email filtering lookup and non-events occurring on any registered FortiGate device which uses the FortiManager system's FDS.

Before you can view lookup and non-event records, you must enable logging for FortiGuard web filtering or email filter events.

To log rating queries:

1. Go to *FortiGuard* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Web Filtering and Email Filter Settings*.
3. Select the log settings:

Log FortiGuard Server Update Events	Enable or disable logging of FortiGuard server update events.
FortiGuard Web Filtering	
Log URL disabled	Disable URL logging.
Log non-URL events	Logs only non-URL events.
Log all URL lookups	Logs all URL lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.

FortiGuard Antispam

Log Spam disabled	Disable spam logging.
Log non-spam events	Logs email rated as non-spam.
Log all Spam lookups	Logs all spam lookups (queries) sent to the FortiManager system’s built-in FDS by FortiGate devices.

FortiGuard Anti-virus Query

Log Virus disabled	Disable virus logging.
Log non-virus events	Logs only non-virus events.
Log all Virus lookups	Logs all virus queries sent to the FortiManager system’s built-in FDS by FortiGate devices.

4. Select *Apply*.

Restoring the URL or antispam database

Formatting the hard disk or partition on FortiManager-3000 units and higher deletes the URL and antispam databases required to provide FortiGuard email filter and web filtering services through the built-in FDS. The databases will re-initialize when the built-in FDS is scheduled next, to synchronize them with the FDN.

Before formatting the hard disk or partition, you can back up the URL and antispam database using the CLI, which encrypts the file. You can also back up licenses as well. The databases can be restored by importing them using the CLI. If you have created a custom URL database, you can also backup or restore this customized database (for FortiGate units).

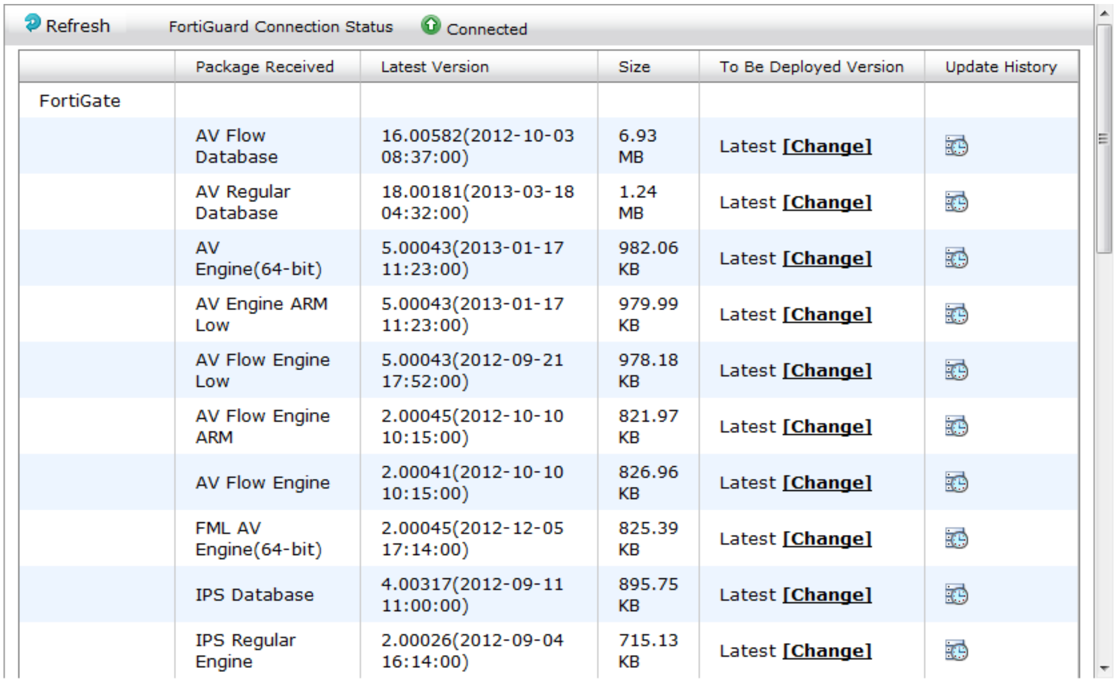
Package management

Antivirus and IPS signature packages are managed in *FortiGuard* > *Package Management*. Packages received from FortiGuard and the service status of managed devices are listed in *Receive Status* and *Service Status*, respectively.

Receive status

To view packages received from FortiGuard, go to
FortiGuard > *Package Management* > *Receive Status*.

Figure 229: FortiGuard package receive status



Refresh FortiGuard Connection Status Connected

	Package Received	Latest Version	Size	To Be Deployed Version	Update History
FortiGate					
	AV Flow Database	16.00582(2012-10-03 08:37:00)	6.93 MB	Latest **[Change]**	
	AV Regular Database	18.00181(2013-03-18 04:32:00)	1.24 MB	Latest **[Change]**	
	AV Engine(64-bit)	5.00043(2013-01-17 11:23:00)	982.06 KB	Latest **[Change]**	
	AV Engine ARM Low	5.00043(2013-01-17 11:23:00)	979.99 KB	Latest **[Change]**	
	AV Flow Engine Low	5.00043(2012-09-21 17:52:00)	978.18 KB	Latest **[Change]**	
	AV Flow Engine ARM	2.00045(2012-10-10 10:15:00)	821.97 KB	Latest **[Change]**	
	AV Flow Engine	2.00041(2012-10-10 10:15:00)	826.96 KB	Latest **[Change]**	
	FML AV Engine(64-bit)	2.00045(2012-12-05 17:14:00)	825.39 KB	Latest **[Change]**	
	IPS Database	4.00317(2012-09-11 11:00:00)	895.75 KB	Latest **[Change]**	
	IPS Regular Engine	2.00026(2012-09-04 16:14:00)	715.13 KB	Latest **[Change]**	

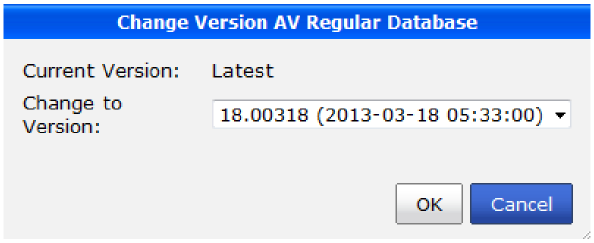
Refresh	Select to refresh the table.
FortiGuard Connection Status	The FortiGuard connection status.
Package Received	The name of the package.
Latest Version	The package version.
Size	The size of the package.
To Be Deployed Version	The package version that is to be deployed. Select Change to change the version. See "Deployed version" on page 291.
Update History	Select the icon to view the package update history. See "Update history" on page 292.

Deployed version

To change the to be deployed version of a received packaged, select *Change* in the *To Be Deployed Version* column for the package.

The *Change Version* dialog box opens, allowing you to select an available version from the drop-down list.

Figure 230: Change deployed package version



Current Version: Latest

Change to Version: 18.00318 (2013-03-18 05:33:00)

Update history

Selecting the update history button in a package's row will open the update history page for that package.

It shows the update times, the events that occured, the statuses of the updates, and the versions downloaded.

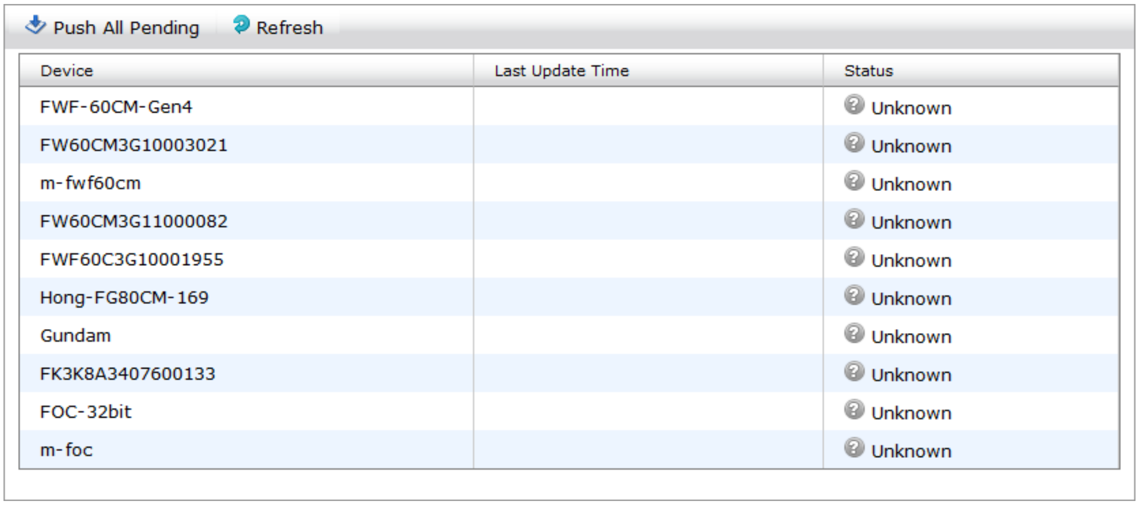
Service status

The service status page shows a list of all the managed FortiGate devices, their last update time, and their status. A device's status can be one of the following:

- OK: the latest package has been received by the FortiGate unit.
- Pending: The FortiGate unit has an older version of the package due to an acceptable reason (such as the scheduled update time having not come yet).
- Problem: The FortiGate unit missed the scheduled query, or did not correctly receive the latest package.
- Unknown: The FortiGate unit's status is not currently known.

Pending updates can also be pushed to the devices, either individually or all at the same time. The list can be refreshed by selecting *Refresh* in the toolbar.

Figure 231: Package service status



Device	Last Update Time	Status
FWF-60CM-Gen4		Unknown
FW60CM3G10003021		Unknown
m-fwf60cm		Unknown
FW60CM3G11000082		Unknown
FWF60C3G10001955		Unknown
Hong-FG80CM-169		Unknown
Gundam		Unknown
FK3K8A3407600133		Unknown
FOC-32bit		Unknown
m-foc		Unknown

To push updates to a device or devices:

1. Go to *FortiGuard* > *Package Management* > *Service Status*.

2. Select *Push All Pending* in the toolbar, or right-click and select *Push All Pending* from the pop-up menu, to push all the pending packages to their devices.

   Select a device, then right-click and select *Push Pending* from the pop-up menu to push the pending package to that device.

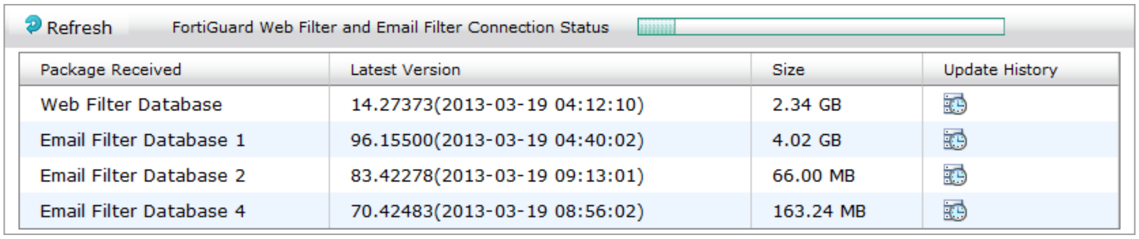
Query server management

The query server manager shows when updates are received from the server, the update version, the size of the update, and the update history. It also has graphs showing the number of queries from all the managed FortiGate units made to the FortiManager device.

Receive status

The view the received packages , go to *FortiGuard < Query Server Management > Receive Status*.

Figure 232: Query receive status



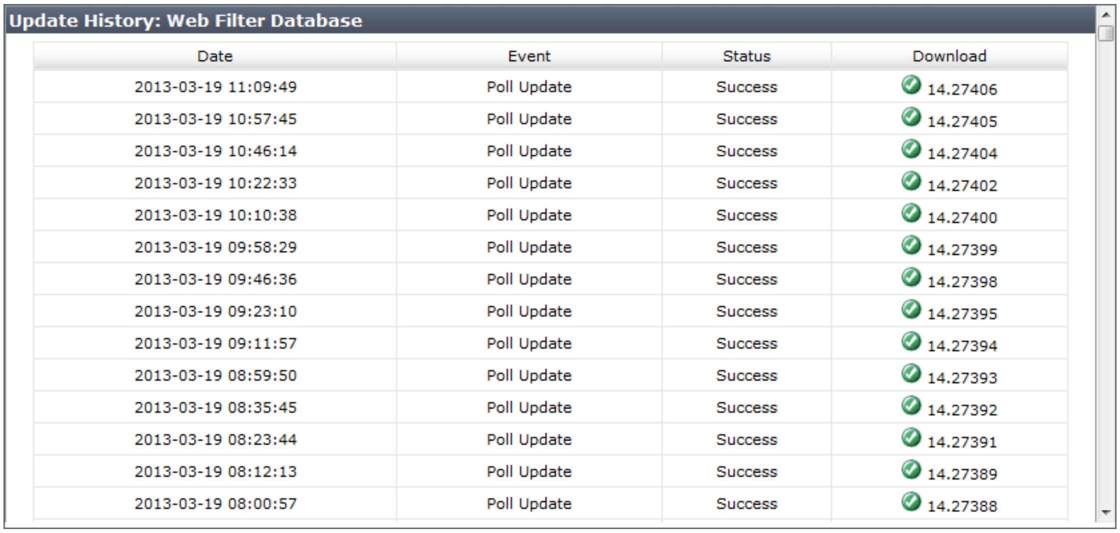
Package Received	Latest Version	Size	Update History
Web Filter Database	14.27373(2013-03-19 04:12:10)	2.34 GB	
Email Filter Database 1	96.15500(2013-03-19 04:40:02)	4.02 GB	
Email Filter Database 2	83.42278(2013-03-19 09:13:01)	66.00 MB	
Email Filter Database 4	70.42483(2013-03-19 08:56:02)	163.24 MB	

Refresh	Select to refresh the table.
Status	The *FortiGuard Web Filter and Email Filter Connection Status*.
Package Received	The name of the received package.
Latest Version	The latest version of the received package.
Size	The size of the package.
Update History	Select to view the package update history. See "Update history" on page 293.

Update history

Selecting the update history button for a package opens the update history page for that package.

Figure 233: Package update history



Update History: Web Filter Database

Date	Event	Status	Download
2013-03-19 11:09:49	Poll Update	Success	✓ 14.27406
2013-03-19 10:57:45	Poll Update	Success	✓ 14.27405
2013-03-19 10:46:14	Poll Update	Success	✓ 14.27404
2013-03-19 10:22:33	Poll Update	Success	✓ 14.27402
2013-03-19 10:10:38	Poll Update	Success	✓ 14.27400
2013-03-19 09:58:29	Poll Update	Success	✓ 14.27399
2013-03-19 09:46:36	Poll Update	Success	✓ 14.27398
2013-03-19 09:23:10	Poll Update	Success	✓ 14.27395
2013-03-19 09:11:57	Poll Update	Success	✓ 14.27394
2013-03-19 08:59:50	Poll Update	Success	✓ 14.27393
2013-03-19 08:35:45	Poll Update	Success	✓ 14.27392
2013-03-19 08:23:44	Poll Update	Success	✓ 14.27391
2013-03-19 08:12:13	Poll Update	Success	✓ 14.27389
2013-03-19 08:00:57	Poll Update	Success	✓ 14.27388

Date	**The date and time of the event.**
Event	**The event that occured.**
Status	**The status of the event.**
Download	**The status of the download and the version number.**

Query status

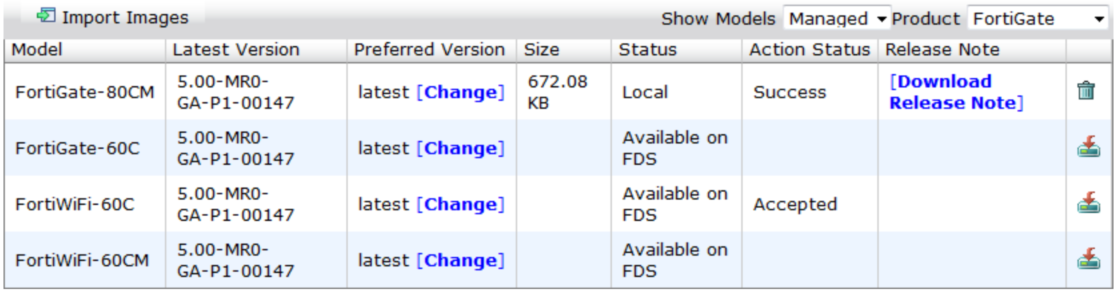
Go to *FortiGuard* > *Query Server Management* > *Query Status* to view graphs that show: the number of queries made from all managed FortiGate devices to the FortiManager unit over a user selected time period, the top ten unrated sites, and the top ten devices for a user selected time period.

Firmware images

Go to *FortiGuard* > *Firmware Images* to manage the firmware images stored on the FortiManager device.

You can download only those images that are needed from the FDS systems, and customize which firmware images are available for deployment.

Figure 234: Firmware images list



Import Images   Show Models: Managed   Product: FortiGate

Model	Latest Version	Preferred Version	Size	Status	Action Status	Release Note	
FortiGate-80CM	5.00-MR0-GA-P1-00147	latest [Change]	672.08 KB	Local	Success	[Download Release Note]	🗑
FortiGate-60C	5.00-MR0-GA-P1-00147	latest [Change]		Available on FDS			⬇
FortiWiFi-60C	5.00-MR0-GA-P1-00147	latest [Change]		Available on FDS	Accepted		⬇
FortiWiFi-60CM	5.00-MR0-GA-P1-00147	latest [Change]		Available on FDS			⬇

Import Images	Select to open the firmware image import list. See “To import a firmware image:” on page 296.
Show Models	From the drop-down list, select *All* to show all the available models on the FortiGuard server, or select *Managed* to show only the models that are currently being managed by the FortiManager device.
Product	Select a managed product type from the drop-down list.
Model	The device model number that the firmware is applicable to.
Latest Version	The latest version of the firmware that is available.
Preferred Version	The firmware version that you would like to use on the device. Select *Change* to open the *Change Version* dialog box, then select the desired version from the drop-down list and select *OK* to change the preferred version.
Size	The size of the firmware image.
Action Status	The status of the current action being taken.
Release Notes	A link to a copy of the release for the formware image that has been dowloaded.
Download/Delete	Download the formware image from the FDS if it is available. If the firmware images has already been downloaded, then delete the firmware image from the FortiManager device.

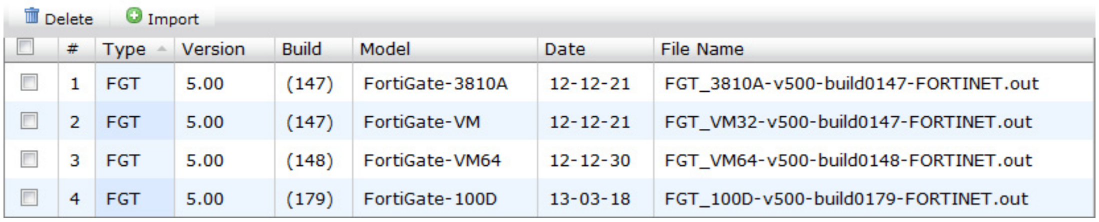
For information about upgrading your FortiManager device, see “FortiManager Firmware” on page 306.

To import a firmware image:

1. Go to *FortiGuard > Firmware Images* and select *Import Images* in the toolbar.

   A list of the currently imported firmware images opens.

   Figure 235: Local firmware images



□	#	Type	Version	Build	Model	Date	File Name
□	1	FGT	5.00	(147)	FortiGate-3810A	12-12-21	FGT_3810A-v500-build0147-FORTINET.out
□	2	FGT	5.00	(147)	FortiGate-VM	12-12-21	FGT_VM32-v500-build0147-FORTINET.out
□	3	FGT	5.00	(148)	FortiGate-VM64	12-12-30	FGT_VM64-v500-build0148-FORTINET.out
□	4	FGT	5.00	(179)	FortiGate-100D	13-03-18	FGT_100D-v500-build0179-FORTINET.out

2. Select *Import* from the toolbar.
3. In the *Upload Firmware Image* dialog box, select *Browse* to browse to the desired firmware image file.
4. Select *OK* to import the firmware image.

Firmware images can be downloaded from the Fortinet Customer Service & Support site at https://support.fortinet.com/ (support account required).

To delete firmware images:

1. Go to *FortiGuard > Firmware Images* and select *Import Images* in the toolbar.
2. Select the firmware images you would like to delete.
3. Select the *Delete* toolbar icon. A confirmation dialog box appears.
4. Select *OK* to delete the firmware images.

High Availability

This section provides a general description of FortiManager High Availability (HA). This section also describes all HA configuration options and includes some basic HA configuration and maintenance procedures.

This section describes:

- HA overview
- Configuring HA options
- Monitoring HA status
- Upgrading the FortiManager firmware for an operating cluster

HA overview

FortiManager high availability (HA) provides a solution for a key requirement of critical enterprise management and networking components: enhanced reliability. Understanding what's required for FortiManager reliability begins with understanding what normal FortiManager operations are and how to make sure that these normal operations continue if a FortiManager unit fails.

Most of the FortiManager operations involve storing FortiManager, and FortiGate configuration and related information in the FortiManager database on the FortiManager unit hard disk. A key way to enhance reliability of FortiManager is to protect the data in the FortiManager database from being lost if the FortiManager unit fails. This can be achieved by dynamically backing up FortiManager database changes to one or more backup FortiManager units. Then if the operating FortiManager unit fails, a backup FortiManager unit can take the place of the failed unit.

A FortiManager HA cluster consists of up five FortiManager units of the same FortiManager model. One of the FortiManager units in the cluster operates as a primary or master unit and the other one to four units operate as backup units. All of the units are visible on the network. The primary unit and the backup units can be at the same location. FortiManager HA also supports geographic redundancy so the primary unit and backup units can be in different locations attached to different networks as long as communication is possible between them (for example over the Internet, over a WAN, or through a private network).

Administrators connect to the primary unit Web-based Manager or CLI to perform FortiManager operations. 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.

A reboot of the FortiManager device is not required when it is promoted from a slave to the master.

Synchronizing the FortiManager configuration and HA heartbeat

All changes to the FortiManager database are saved on the primary unit, and then these changes are synchronized to the backup units. The FortiManager configuration of the primary unit is also synchronized to the backup units (except for the HA parameters). 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.

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.

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

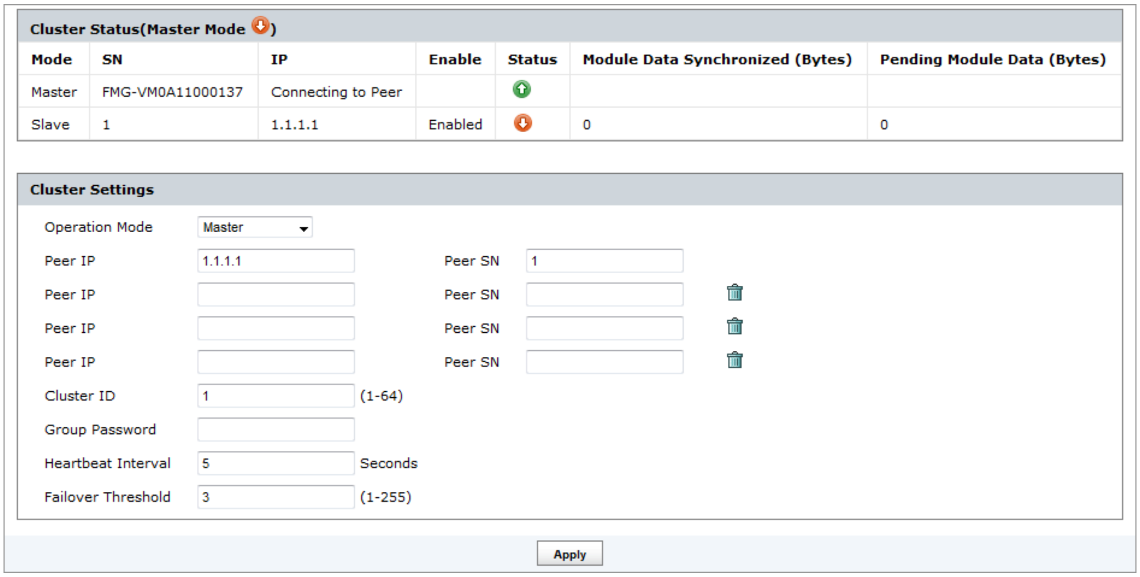
To configure HA options go to *System Settings* > *General* > *HA*. From here you can configure FortiManager units to start an HA cluster or you can change the HA configuration of the cluster.

To configure a cluster, you must set the mode of the primary unit to Master and the modes of the backup units to Slave.

Then you must add the IP addresses and serial numbers of each backup unit to primary unit peer list. The IP address and serial number of the primary unit must be added to each of the backup unit HA configurations. Also, the primary unit and all backup units must have the same *Cluster ID* and *Group Password*.

You can connect to the primary unit 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.

Figure 236: Cluster settings



Cluster Status(Master Mode ⬇)

Mode	SN	IP	Enable	Status	Module Data Synchronized (Bytes)	Pending Module Data (Bytes)
Master	FMG-VM0A11000137	Connecting to Peer		⬆		
Slave	1	1.1.1.1	Enabled	⬇	0	0

Cluster Settings

Operation Mode	Master			
Peer IP	1.1.1.1	Peer SN	1	
Peer IP		Peer SN		🗑
Peer IP		Peer SN		🗑
Peer IP		Peer SN		🗑
Cluster ID	1	(1-64)		
Group Password				
Heartbeat Interval	5	Seconds		
Failover Threshold	3	(1-255)		

Cluster Status	Monitor FortiManager HA status. See "Monitoring HA status" on page 304.
Mode	The high availability mode, either *Master* or *Slave*.
SN	The serial number of the device.
IP	The IP address of the device.
Enable	Shows if the peer is currently enabled.
Status	The status of the cluster member.
Module Data Synchronized	Module data synchronized represented in Bytes.
Pending Module Data	Pending module data represented in Bytes.
Cluster Settings	
Operation Mode	Select *Master* to configure the FortiManager unit to be the primary unit in a cluster. Select *Slave* to configure the FortiManager unit to be a backup unit in a cluster. Select *Standalone* to stop operating in HA mode.
Peer IP	Enter the IP address of another FortiManager unit in the cluster. For the primary unit you can add up to four Peer IPs for up to four 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 four Peer serial numbers for up to four backup units. For a backup unit you add the serial number of the primary unit.

Cluster 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. Sample configuration settings are also shown.

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.

   Example HA master configuration:

Operation Mode	Master
Peer IP	172.20.120.23
Peer SN	<serial_number>
Peer IP	192.268.34.23
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
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.

   Example local backup configuration:

Operation Mode	Slave
Priority	5 (Keep the default setting.)
Peer IP	172.20.120.45
Peer SN	<serial_number>
Cluster ID	15
Group Password	password

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.

   Example remote backup configuration:

Operation Mode	Slave
Priority	5 (Keep the default setting.)
Peer IP	192.168.20.23
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
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:

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.

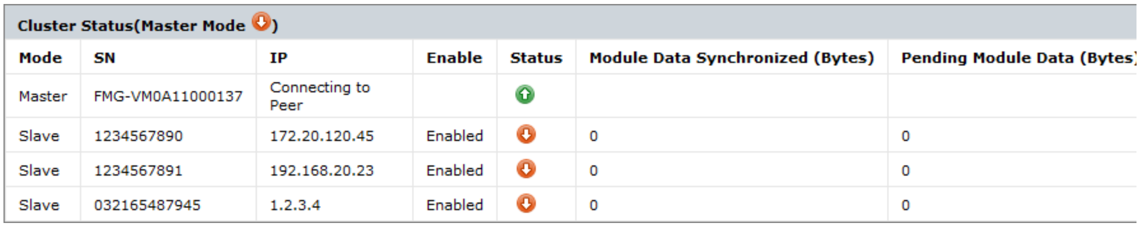
Monitoring HA status

Go to *System Settings* > *General* > *HA* to monitor the status of the FortiManager units in an operating HA cluster. The FortiManager HA status dialog box displays information about the role of each cluster unit, the HA status of the cluster, and also displays the HA configuration of the cluster.

The FortiManager 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.

From the FortiManager CLI you can use the command `get system ha` to display the same HA status information.

Figure 237: FortiManager HA status



Cluster Status(Master Mode ⬇)

Mode	SN	IP	Enable	Status	Module Data Synchronized (Bytes)	Pending Module Data (Bytes)
Master	FMG-VM0A11000137	Connecting to Peer		⬆		
Slave	1234567890	172.20.120.45	Enabled	⬇	0	0
Slave	1234567891	192.168.20.23	Enabled	⬇	0	0
Slave	032165487945	1.2.3.4	Enabled	⬇	0	0

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 was a upgrading the firmware of a standalone FortiManager unit. During the firmware upgrade procedure, you connect to the primary unit Web-based Manager or CLI to upgrade the firmware. Then install the firmware on the slave units.

Similar to upgrading the firmware of a standalone FortiManager unit, normal FortiManager operations are temporarily interrupted while the cluster firmware upgrades. As a result of this interruption, you should upgrade the firmware during a quiet period.

To upgrade FortiManager HA cluster firmware:

1. Log into the primary unit Web-based Manager.
2. Upgrade the primary unit firmware.

   The firmware is forwarded to all the slave units, and then all the devices (master and slaves) are rebooted.

   See "FortiManager Firmware" on page 306 for more information.

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.

FortiManager Firmware

This section explains how to properly upgrade to FortiManager v5.0 Patch Release 2. The following topics are included in this section:

- Upgrading from FortiManager v5.0.0
- Upgrading from FortiManager v4.0 MR3
- Downgrading to previous firmware versions

Upgrading from FortiManager v5.0.0

FortiManager v5.0 Patch Release 2 officially supports upgrade from FortiManager v5.0.0 or later.

General firmware upgrade steps

The following table lists the general firmware upgrade steps.

Table 13: Upgrade steps

Step 1	Prepare your FortiManager for upgrade.
Step 2	Backup your FortiManager system configuration.
Step 3	Transfer the FortiManager v5.0 Patch Release 2 firmware image to your FortiManager device.
Step 4	Log into your FortiManager Web-based Manager to verify the upgrade was successful.

Step 1: Prepare your FortiManager for upgrade

1. Install any pending configurations.
2. Make sure all managed FortiGate devices are running FortiOS v4.0 MR2/v4.0 MR3 or FortiOS v5.0.0 or later.

Step 2: Backup your FortiManager system configuration

1. Login to your FortiManager v5.0.0 Web-based Manager.
2. Go to *System Settings* > *General* > *Dashboard*.
3. Select *Backup* on the *System Information* widget.
4. Back up the system configuration; save the configuration file (.dat file) to your local computer.

Step 3: Transfer the firmware image to your FortiManager device

Transfer the new FortiManager v5.0 Patch Release 2 firmware image to your FortiManager device:

1. Login to the FortiManager v5.0.0 Web-based Manager.
2. Go to *System Settings* > *General* > *Dashboard*.

3. Select *Update* on the *System Information* widget.
4. Browse for FortiManager v5.0 Patch Release 2 image file on your local computer.
5. Select *OK*.

After the upgrade, please clear your browser cache before logging into the FortiManager Web-based Manager. Please make sure your computer's screen resolution is set to at least 1280x1024, otherwise the Web-based Manager may not be displayed properly.

Step 4: Verify the upgrade

1. Login to the FortiManager Web-based Manager using the previously configured administrator name and password. Review all administrator profiles to configure the proper access privileges.
2. Launch the *Device Manager* module and make sure that all formerly added FortiOS v4.0 MR2/MR3 and FortiOS v5.0.0 or later devices are still listed.
3. Launch other functional modules and make sure they work properly.

Upgrading from FortiManager v4.0 MR3

FortiManager v5.0 Patch Release 2 officially supports upgrade from FortiManager v4.0 MR3.

General firmware upgrade steps

The following table lists the general firmware upgrade steps.

Table 14: Upgrade steps

Step 1	Prepare your FortiManager for upgrade.
Step 2	Backup your FortiManager system configuration.
Step 3	Transfer the FortiManager v5.0 Patch Release 2 firmware image to your FortiManager device.
Step 4	Log into your FortiManager Web-based Manager to verify the upgrade was successful.

Step 1: Prepare your FortiManager for upgrade

1. Install any pending configurations.
2. Upgrade your FortiManager to at least v4.0 MR3. For more information, see the *FortiManager v4.0 MR3 Release Notes* for the upgrade procedure.
3. Make sure all managed FortiGate devices are running FortiOS v4.0 MR2 or v4.0 MR3.

Step 2: Backup your FortiManager system configuration

1. Login to your FortiManager v4.0 MR3 Web-based Manager.
2. Go to *System Settings* > *General* > *Dashboard*.

3. Select *Backup* on the *System Information* widget.
4. Back up the system configuration; save the configuration file (.dat file) to your local computer.

The system configuration file from a FortiManager v4.0 MR3 device cannot be directly imported into a FortiManager v5.0 Patch Release 2 device.

Step 3: Transfer the firmware image to your FortiManager device

Transfer the new FortiManager v5.0 Patch Release 2 firmware image to your FortiManager device:

1. Login to the FortiManager v4.0 MR3 Web-based Manager.
2. Go to *System Settings* > *General* > *Dashboard*.
3. Select *Update* on the *System Information* widget.
4. Browse for FortiManager v5.0 Patch Release 2 image file on your local computer.
5. Select *OK*.

After the upgrade, please clear your browser cache before logging into the FortiManager Web-based Manager. Please make sure your computer's screen resolution is set to at least 1280x1024, otherwise the Web-based Manager may not be displayed properly.

Step 4: Verify the upgrade

1. Login to the FortiManager Web-based Manager using the previously configured administrator name and password. Review all administrator profiles to configure the proper access privileges.
2. Launch the *Device Manager* module and make sure that all formerly added FortiOS v4.0 MR2 and MR3 devices are still listed.
3. Launch other functional modules and make sure they work properly.

Downgrading to previous firmware versions

FortiManager v5.0 Patch Release 2 does not provide a full downgrade path. For those users who want to downgrade to an older FortiManager firmware release, downgrade the system firmware via a TFTP server with the firmware burning procedure embedded within the FortiManager system boot-up menu. A full format of the system hard drives and system reset are required after the firmware downgrading process.

All configuration will be lost after downgrading the device, and the system hard drives will be formatted.

To re-initialize a FortiManager use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format disk
```

Appendix A: FortiManager VM

FortiManager VM system requirements

The following table provides a detailed summary on FortiManager VM system requirements.

Table 15: FortiManager VM system requirements

Virtual Machine	Requirement
Hypervisor Support	VMware ESXi / ESX 4.0, 4.1, 5.0 and 5.1
Virtual Machine Form Factor	Open Virtualization Format (OVF)
Virtual CPUs Supported (Minimum / Maximum)	1 / Unlimited
Virtual NICs Supported (Minimum / Maximum)	1 / 4
Storage Support (Minimum / Maximum)	80GB / 16TB
Memory Support (Minimum / Maximum)	1GB / 4GB for 32-bit and 1GB / unlimited for 64-bit
High Availability Support	Yes

Appendix B: Maximum Values

FortiManager maximum values

The following table provides a detailed summary of maximum values on FortiManager platforms.

Table 16: FortiManager Maximum Values

FortiManager Platform	Devices	Max ADOMs	Max Web Portal / Users
FMG-200D	30	30	-
FMG-400C	300	300	-
FMG-1000C	800	800	800
FMG-3000C	5000	5000	5000
FMG-5001A	4000	4000	4000
FMG-VM-Base	10	10	10
FMG-VM-10	+10	+10	+10
FMG-VM-100	+100	+100	+100
FMG-VM-1000	+1000	+1000	+1000
FMG-VM-5000	+5000	+5000	+5000
FMG-VM-U	Unlimited	Unlimited	Unlimited

Index