FortiManager - Administration Guide

VERSION 5.2.3

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com

July 31, 2015

FortiManager 5.2.3 Administration Guide

02-523-232175-20150731

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-07-31	Initial release

Introduction

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

FortiManager features

FortiManager provides the following features:

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

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

FortiManager feature set

The FortiManager feature set includes the following modules:

- Device Manager
- Policy & Objects
- FortiGuard
- System Settings

FortiAnalyzer feature set

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

- FortiView (FortiView & Log View)
- Event Management
- Reports

About this document

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

The FortiManager documentation assumes that you have one or more FortiGate units, 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 Administration Guide*

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

- *FortiManager device QuickStart Guides*

  These documents are included with your FortiManager system package. Use these document to install and begin working with the FortiManager system and FortiManager Graphical User Interface (GUI).

- *FortiManager Online Help*

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

- *FortiManager CLI Reference*

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

- *FortiManager Release Notes*

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

- *FortiManager VM Install Guide*

  This document describes installing FortiManager VM in your virtual environment.

What's New in FortiManager version 5.2

FortiManager version 5.2 includes the following new features and enhancements. Always review all sections in the *FortiManager Release Notes* prior to upgrading your device.

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

FortiManager version 5.2.2

FortiManager version 5.2.2 includes the following new features and enhancements.

- Create device groups from the Task Monitor.
- Progress bar added to the upgrade status display.
- LDAP Browse added.
- Multicast Policy Support at the ADOM level added.

FortiManager version 5.2.1

FortiManager version 5.2.1 includes the following new features and enhancements.

- Toolbar buttons for the Policy section.
- Install for admin with Restricted profile.
- Approval matrix for Workflow.
- IPv6 support for FG-FM connections.
- Unify JSON APIs with XML APIs.
- Added version to JSON APIs for Policy Package & Objects.
- Common ADOM version for FortiOS v5.0 and v5.2.
- A message is displayed when the database is upgrading or rebuilding. The message contains the estimated time to complete the action.
- Optional dynamic VIP default values.

FortiManager version 5.2.0

FortiManager version 5.2.0 includes the following new features and enhancements.

Workflow mode

Workflow mode is a new global mode to define approval or notification workflow when creating and installing policy changes. Workflow mode is enabled via the CLI only. When workflow mode is enabled, the admin will have

a new option in the admin profile page to approve/reject workflow requests.

For administrators with the appropriate permissions, they will be able to approve or reject any pending requests. When viewing the session list, they can choose any sessions that are pending and click the approve/reject buttons. They can add a note to the approval/rejection response. The system will send a notification to the admin that submitted the session. If the session was approved, no further action is required. If the session was rejected, the admin will need to log on and repair their changes. Once they create a session, the admin will make their repair on top of the last session changes.

When you want to start a workflow, go to the *Policy & Objects* tab, select the ADOM from the drop-down list, lock the ADOM, and click the *Start Session* button. You can then proceed to make changes to policies and objects. When you are done making changes, click the *Save* button and then the *Submit* button. Once the session is submitted, the lock is released and other administrators may initiate a session.

The session list allows user to view any pending requests for approval or active sessions. The session list displays details of each session and allows you to browse the changes performed for the selected session.

To enable and disable workflow mode:

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

```
config system global
   set workspace-mode {workflow | disabled}
end
```

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

When `workspace-mode` is `workflow`, the Device Manager tab and *Policy & Objects* tab are read-only. You must lock the ADOM to start a workflow session.

Advanced CLI-Only Objects menu

An advanced *CLI-Only Objects* menu has been added in the Device Manager and *Policy & Objects* tabs which allows you to configure device settings which are normally configured via the at the CLI on the device. This menu includes commands which are only available in the CLI.

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

VPN Monitor menu in Device Manager

A VPN monitor tree menu has been added to provide real-time VPN status information including which users are connected to the FortiGate selected. The menu contains a Central IPsec and a Central SSL-VPN monitor. For IPsec VPN, you can select to bring the tunnel up or down using the right-click menu.

FortiToken two-Factor authentication for admin log in

FortiManager now supports FortiToken two-factor authentication for administrator logon. When creating a new administrator, select *Type* > *RADIUS*, and select the FortiAuthenticator server in the RADIUS server drop-down list. FortiToken is authenticated via FortiAuthenticator. When configured, the user will be prompted to type the FortiToken code after entering their user name and password.

Successful authentication will provide the user with permission to the FortiManager and will generate a logon event log on the FortiAuthenticator.

UUID support

In FortiOS version 5.2, a universally unique identifier (UUID) attribute has been added to some firewall objects, so that the logs can record these UUIDs to be used by a FortiManager or FortiAnalyzer unit. When installing a configuration to a FortiOS v5.2 device, a single UUID is used for the same object or policy across all managed FortiGates.

In the *FortiView* > *Log View* tab, you can select a log entry, right-click, and select *Jump to Policy* from the pop-up menu to view the policy associated with the log message. In the *Policy & Objects* tab, you can select a policy, right-click, and select *Show Matching Logs* from the pop-up menu to view any logs associated with the policy.

The FortiAnalyzer feature set must be enabled to view the *FortiView* > *Log View* tab.

Dynamic address group

A new option has been added to allow an address group to be a dynamic group. Group mappings can be configured for specific devices.

Dynamic mapping management improvements

The following improvements have been made to dynamic mapping management:

- Convert an address to a dynamic address
- A radio button has been added to allow you to turn dynamic mapping on or off for various firewall objects. When dynamic mapping is enabled, you can view existing mappings or create a new dynamic mapping.
- Dynamic address with mapping table

  In dynamic address mode, the table of mappings is displayed allowing you to add, edit, or delete device mapping. When editing a mapping, the settings are displayed in a pop-up dialog box.

Object GUI enhancements

When creating or editing objects in *Policy & Objects,* a dialog box is displayed similar to the policy dialog box.

Central AP management improvements

Access points that are managed by the FortiGate units managed by the FortiManager device can be configured from the All FortiAP group in the tree menu of the Device Manager tab. In FortiManager v5.2 you can now apply

column filters to organize and drill down the information displayed. The right-click menu now includes options to assign a profile, create new, edit, delete, authorize, deauthorize, upgrade, restart, refresh, view clients, and view rogue APs. You can also assign tags to FortiAPs to make it easier to group and filter devices by the tags.

Improved logging of script execution

FortiManager now includes several logs for scripting functions including: creating scripts, groups, and installing scripts.

Firmware version displayed is consistent with FortiOS

FortiManager v5.2 uses the firmware naming convention '5.2.0', where the first digit reflects the version, the second digit reflects the release, and the third digit reflects the patch. This change is consistent with FortiOS v5.2.0 changes. All references to the firmware version in the GUI and have been updated to this new format.

Update service to FortiWeb

FortiManager v5.2 can now provide antivirus updates to FortiWeb.

FortiExtender support

When adding a FortiGate to FortiManager that is managing a FortiExtender, the FortiExtender will be available in an *All FortiExtender* group in the ADOM. You can authorize, deauthorize, upgrade, restart, edit, and view the status of the FortiExtender from the right-click menu.

Restricted Admin profiles

Create restricted admin profiles to allow a delegated administrator to manage their ADOM's security profiles. You can allow the delegated administrator to make changes to the Web Filter profile, IP sensor, and Application sensor associated with their ADOM.

Flexible FortiGuard Distribution Server (FDS) override list management

The *System Template* now allows you to configure multiple override servers, FortiManager, and FortiGuard servers into one list. You can provide services to FortiGates using this template. When adding new servers, you can select the server type, update, rating or both. This feature allows you to manage FortiGates with different override lists.

Model device improvements

The *Add Model Device* option in the *Device Wizard* has been updated to allow you to provisioning a single device or multiple devices more efficiently. When adding a device, only the FortiGate serial number and FortiOS version are required. A new option has been added to allow you to add multiple devices by importing a Comma Separated Value (CSV) file with the required information.

Once the model device is added to FortiManager you can assign the device to an ADOM, assign a policy package, and associate it with a provisioning template. When an unregistered FortiGate with a matching serial number connects to FortiManager, you can install the model device configuration.

Enable the FortiAnalyzer feature set in the GUI

In FortiManager version 5.0.6 or earlier, the FortiAnalyzer feature set was enabled or disabled via the CLI only. In FortiManager v5.2.0 or later, you can also enable or disable these features in the GUI. To enable the FortiAnalyzer feature set, go to *System Settings* > *Dashboard*. In the *System Information* widget, select *[Enabled]* beside *FortiAnalyzer Features*.

When enabling or disabling FortiAnalyzer Features, your FortiManager will reboot.

FortiSandbox support

FortiSandbox version 1.4 can be centrally managed by a FortiManager running version 5.2.0 or later.

Policy package locking

In FortiManager version 5.2 you can lock and edit a policy package without locking the ADOM. When the policy package is locked, other users are unable to lock the ADOM or edit the locked policy package. The policy package is edited in a private workspace. Only the policy package is in the workspace, not the object database. When locking and editing a policy package, the object database remains locked. The policy package lock status is displayed in the toolbar.

Before you can lock an ADOM or policy package, you must first enable `workspace` to disable concurrent ADOM access from the CLI.

When workspace is enabled, all ADOMs and policy packages are read-only. In the Device Manager tab, you can right-click an ADOM and select *Lock* from the right-click menu. When the ADOM is locked you can edit the ADOM, all other administrators need to wait until you unlock the ADOM.

In the *Policy & Objects* tab, you can select to lock the ADOM from the toolbar. When the ADOM is locked, all policy packages and objects in that ADOM are locked and read-only to other administrators until you finish your edits and unlock the ADOM.

Policy Package locking allows you to lock a specific policy package without locking the ADOM. In the *Policy & Objects* tab, select the ADOM from the drop-down list, select the policy package, right-click and select *Lock & Edit* from the right-click menu.

When a policy package is locked, other administrators are not able to lock the ADOM in the Device Manager or *Policy & Objects* tabs. The policy package is displayed as locked. Other administrators can however lock and edit other policy packages in the same ADOM.

When the policy package is locked, the administrator can edit the policy package as required and access the following options in the left side tree right-click menu: *Install Wizard*, *Export*, *Policy Check*, *Save*, and *Unlock*. Before unlocking the policy package, select *Save* in the toolbar or right-click menu to save changes made to the policy package for the session.

When changes are made to a policy package, the policy package name is highlighted red and the save option is available in the toolbar and right-click menu.

Although another administrator can select to lock and edit an unlocked policy package, neither administrator is able to create a new policy package or edit the object database. To create a new policy package or edit the object database, the ADOM must be locked.

When an ADOM or policy package is locked, the lock is automatically released by an admin idle timeout or by closing the browser window. Any unsaved changes will be lost. Always ensure that changes are saved using the save option in the toolbar or right-click menu.

Import improvements

The following improvements have been made to the import operation:

- Auto resynchronization when tunnel re-up: After changes are made to a FortiGate, when the tunnel comes back online, the changes are auto-synchronized to FortiManager. The device manager database is always in sync with the FortiGate and the out-of-sync condition has been removed.
- Detect FortiGate changes that impact policy & objects: FortiManager now is able to detect when the settings were changed on the FortiGate and synchronized back to the related policy and object settings. This allows you to know when the policy package is out-of-sync with what is installed on the FortiGate. You can either re-apply the changes or modify the policy package.
- Warning when overwrite an existing policy package: FortiManager now displays a warning dialog box allowing you to decide to either overwrite the policy package, cancel the import, or import the policy package under a different name.

Policy & Objects display options improvement

When importing objects or policy types, FortiManager will detect whether or not the related display option is enabled. If it is not, FortiManager will prompt the user via a dialog box to enable the display options item.

Central WiFi management improvements

The following improvements have been made to central WiFi management:

- Wireless Profiles have been renamed Custom AP Profiles
- Created, edit, and delete APs
- Assign AP profiles to multiple APs
- Consistent replacement messages between FortiGate and FortiManager
- Customize Captive Portal messages per SSID.

Central AP management improvements

Access points that are managed by the FortiGate units managed by the FortiManager device can be configured from the All FortiAP group in the tree menu of the Device Manager tab. In FortiManager 5.2.3 you can now apply column filters to organize and drill down the information displayed. The right-click menu now includes options to assign a profile, create new, edit, delete, authorize, deauthorize, upgrade, restart, refresh, view clients, and view rogue APs. You can also assign tags to FortiAPs to make it easier to group and filter devices by the tags.

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, FortiSwitch, and FortiSandbox 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 5 000 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. See Administrative Domains on page 32.

Local FortiGuard service provisioning

A FortiGate device can use the FortiManager unit for antivirus, intrusion prevention, web filtering, and email filtering to optimize performance of rating lookups, and definition and signature downloads. See FortiGuard Management on page 307.

Firmware management

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

Scripting

FortiManager supports CLI or Tcl based scripts to simplify configuration deployments. See Scripts on page 218.

Logging and reporting

FortiManager can also be used to log traffic from managed devices and generate Structured Query Language (SQL) based reports. FortiManager also integrates FortiAnalyzer logging and reporting features.

Fortinet device life cycle management

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

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

Inside the FortiManager system

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

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. See Device Manager on page 128.

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. See Policy & Objects on page 248.

System Settings tab

The *Systems Settings* tab enables the configuration of system settings and monitors the operation of your FortiManager unit. See System Settings on page 44.

Inside the FortiManager device manager tab

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 GUI

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

This section includes the following topics:

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

System requirements

Supported web browsers

The following web browsers are supported by FortiManager 5.2.3:

- Microsoft Internet Explorer version 11
- Mozilla Firefox version 33
- Google Chrome version 38

Other web browsers may function correctly, but are not supported by Fortinet. For more information see the *FortiManager Release Notes*.

Monitor settings for GUI access

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

Connecting to the GUI

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

To connect to the GUI:

1. Connect the 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:
   - Browse to *Network and Sharing Center* > *Change Adapter Settings* > *Local Area Connection Properties* > *Internet Protocol Version 4 (TCP/IPv4) Properties*.
   - 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 GUI, start an Internet browser of your choice and browse to `https://192.168.1.99`.
4. Type admin in the *Name* box, leave the *Password* box 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 69.

If the URL is correct and you still cannot access the GUI, you may also need to configure static routes. For details, see Configuring static routes on page 70.

When the system is busy during a database upgrade or rebuild, you will receive a message in the GUI log in screen. The message will include the estimated completion time.

GUI overview

FortiManager v5.2 introduces an improved GUI layout and tree menu for improved usability. You can now select the ADOM from the drop-down list to view the devices and groups for the specific ADOM. The ADOM selection drop-down list is available in the *Device Manager*, *Policy & Objects*, FortiView, Event Management, and Reports tabs.

This section describes the following topics:

Viewing the GUI

The four main parts of the FortiManager GUI are the tree menu, tab bar, ADOM selector and toolbar, and right content pane.

The GUI includes detailed online help. Selecting *Help* in the tab bar opens the online help.

The tab bar 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 administrator profiles, go

to *System Settings* > *Admin* > *Profile*. You can configure the administrator profile at both a global and ADOM level with a high degree of granularity in providing read/write, read-only, or restricted permission to various GUI 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 permissions, see Admin on page 74.

When you log in to the FortiManager unit as the `admin` administrator, the GUI 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 128.

Configuration changes made using the GUI take effect immediately without resetting the FortiManager system or interrupting service.

Using the tab bar

The tab bar is organized into a number of tabs. The available tabs displayed are dependent on the features enabled and the administrator profile settings.

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. In the Menu section, you can configure managed devices locally in the FortiManager GUI. In the Provisioning Templates section, you can configure System Templates, WiFi Templates, Threat Weight Templates, FortiClient Templates, and Certificate Templates and assign these templates to specific managed FortiGate and FortiCarrier devices. Additional menus are available for scripts and VPN monitor. For more information, see Device Manager on page 128.
Policy & Objects	Configure policy packages and objects. When Central VPN Console is enabled for the ADOM, you can create VPN topologies and managed/external gateways. For more information, see Policy & Objects on page 248.
FortiGuard	Configure FortiGuard Center settings, package and query server management, and firmware images. For more information, see FortiGuard Management on page 307.
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 44.

Tab	Description
FortiView	The following summary views are available: Top Sources, Top Applications, Top Destinations, Top Websites, Top Threats, Top Cloud Applications, Top Cloud Users, System Events, Admin Logins, SSL & Dialup IPsec, Site-Site IPsec, Rogue APs, and Resource Usage. This tab was implemented to match the FortiView implementation in FortiGate. The *Log View* tab is found in the FortiView tab. View logs for managed devices. You can display, download, import, and delete logs on this page. You can also define Custom Views. This tab can be hidden by disabling the FortiAnalyzer feature set.
Event Management	Configure and view events for managed log devices. You can view events by severity or by handler. For more information, see Event Management on page 374. This tab can be hidden by disabling the FortiAnalyzer feature set.
Reports	Configure report templates, schedules, and output profiles. You can create and test datasets, configure output profiles, and add language support. For more information, seeReports on page 385. This tab can be hidden by disabling the FortiAnalyzer feature set.

Configuring GUI settings

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

This section includes the following topics:

Changing the GUI language

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

To change the GUI language:

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

Administrative access

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

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

HTTPS	PING	TELNET	Web Service
HTTP	SSH	SNMP	

To change administrative access to your FortiManager system:

1. Go to *System Settings* > *Network*.
   Administrative access is configured for port1. To configure administrative access for another interface, 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 earlier, you can select to enable access on interface from the *All Interfaces* window.

Restricting GUI access by trusted host

To prevent unauthorized access to the GUI you can configure administrator accounts with trusted hosts. With trusted hosts configured, the administrator user can only log into the GUI when working on a computer with the trusted host as defined in the administrator account. You can configure up to ten trusted hosts per administrator account. See Administrator on page 75 for more details.

Changing the GUI idle timeout

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

To change the GUI idle timeout:

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

Other security considerations

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

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

Reboot and shutdown of the FortiManager unit

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

To reboot the FortiManager unit:

1. From the GUI, go to *System Settings* > *Dashboard*.
2. In the Unit Operation widget select *Reboot*, or from the CLI Console widget type:
```
execute reboot
```

To shutdown the FortiManager unit:

1. From the GUI, go to *System Settings* > *Dashboard*.
2. In the Unit Operation widget select *Shutdown*, or from the CLI Console widget type:
```
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.

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

This section includes the following topics:

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

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

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

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

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.
	ADOMs must be enabled to support FortiMail and FortiWeb logging and reporting. When a FortiMail or FortiWeb device is promoted to the DVM table, the device is added to their respective default ADOM and will be visible in the left-hand tree menu.
	FortiGate and FortiCarrier devices cannot be grouped into the same ADOM. FortiCarrier devices are added to a specific default FortiCarrier ADOM.

To enable the ADOM feature:

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

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* > *Dashboard.*
4. In the system information widget, select *Disable* next to *Administrative Domain.*

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 permission. 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 GUI 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.

ADOM versions

ADOMs can concurrently manage FortiGate units running both FortiOS v4.3 and v5.0, or v5.0 and v5.2, allowing devices running these versions to share a common database. This allows you to continue to manage an ADOM as normal while upgrading the devices within that ADOM.

This feature should only be used to facilitate upgrading to new firmware. ADOMs should not be regularly run in this mode.

FortiManager v5.2 supports FortiOS v4.3, v5.0, and v5.2 ADOMs. For a complete list of supported devices and firmware versions, see the FortiManager Release Notes.

Each ADOM is associated with a specific FortiOS version, based on the firmware version of the devices that are in that ADOM. This version is selected when creating a new ADOM (see Adding an ADOM on page 36), and can be updated after the all of the devices within the ADOM have been updated to the latest FortiOS firmware version.

The general steps for upgrading an ADOM that contains multiple devices running FortiOS v4.3 from v4.3 to v5.0 are as follows:

1. Make sure that the FortiManager unit is upgraded to a version that supports this feature.
2. In the ADOM, upgrade one of the FortiGate units to FortiOS v5.0, and then resynchronize the device.
3. All the ADOM objects, including Policy Packages, remain as v4.3.
4. Upgrade the rest of the FortiGate units in the ADOM to version 5.0 firmware.

5. Upgrade the ADOM to v5.0. See Upgrading an ADOM on page 37 for more information.
   All of the database objects will be converted the v5.0 format, and the GUI content for the ADOM will change to reflect the v5.0 features and behavior.

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

In FortiManager v5.2.1 or later, FortiOS v5.0 and v5.2 share a common policy package database. You can upgrade a v5.0 ADOM to v5.2.

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* > *All ADOMs*. See All ADOMs on page 61 for more information.

Extend workspace to entire ADOM

When concurrent ADOM access is disabled, administrators are able to lock the ADOM. A right-click menu option has been added to allow you to lock/unlock ADOM access; see Locking an ADOM on page 39. The ADOM lock status is displayed by a lock icon to the left side of the ADOM name. FortiManager 5.0.6 adds the ability to lock and edit the policy package independent from the ADOM lock.

The lock status is as follows:

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

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

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

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

Workspace is disabled by default, and is enabled in 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 permission 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 permission. 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 type the following CLI command lines:

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

To disable ADOM locking and enable concurrent ADOM access type the following CLI command lines:

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

Use this command for both ADOM and Policy Package locking.

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 GUI; see To enable the ADOM feature: on page 33.

To create an ADOM

1. Do one of the following:
   - Go to the *Device Manager* tab and select Manage ADOMs from the ADOM drop-down list. Select *Create New* in the *Manage ADOMs* toolbar.
   - Go to *System Settings* > *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.
2. Configure the following settings:

Name	Type a name that will allow you to distinguish this ADOM from your other ADOMs. ADOM names must be unique.
Device Type	Select either FortiGate or FortiCarrier from the drop-down menu. Other devices types are added to their respective default ADOM upon registering with FortiManager.

Version	Select the version of FortiGate devices in the ADOM. FortiManager v5.2 supports FortiOS v5.2, v5.0, and v4.3. For information on supported device firmware version, see the *FortiManager Release Notes*.
Mode	Select *Normal* mode if you want to manage and configure the connected FortiGate devices from the FortiManager GUI. Select *Backup* mode if you want to backup the FortiGate configurations to the FortiManager, but configure each FortiGate locally.
VPN Management	Select *Central VPN Console* or select *Policy & Device VPNs*. When *Central VPN Console* is selected, the *VPN Console* menu item will be visible under the *Policy & Objects* tab. You can configure VPN topologies and managed/external gateway objects. When *Policy & Device VPNs* is selected, VPN configuration is done individually on each FortiGate device.
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 *Specify Devices/Groups*.

3. Select *OK* to create the ADOM.

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

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.

In the confirmation dialog box, select *OK*.

Upgrading an ADOM

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

An ADOM can only be upgraded after all the devices within the ADOM have been upgraded. See ADOM versions on page 34 for more information.

To upgrade an ADOM:

1. Go to the *System Settings* tab and select *All ADOMs*.
2. Right click the ADOM you would like to upgrade from the ADOM list in the content pane and select *Upgrade* from the pop-up menu.

   If the ADOM has already been upgraded to the latest version, this option will not be available.
3. Select *OK* in the confirmation dialog box to upgrade the device.

   If all of the devices within the ADOM are not already upgraded to 5.0, the upgrade will be aborted and a warning dialog box will be shown. Select *OK* in the dialog box, upgrade the remaining devices within the ADOM, and return to step 1 to try upgrading the ADOM again.

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, in the ADOM drop-down menu, select Manage ADOMs. Select the ADOM you want to edit, right-click and 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.
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 control key while selecting each additional device.

You can add devices, device groups, and provision devices using the FortiManager wizards. For more information, see FortiManager Wizards on page 202.

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 38.

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.

Locking an ADOM

If workspace is enabled, you must lock an ADOM prior to performing any management tasks on it. An ADOM can be locked from either the *Device Manager* tab or the *Policy & Objects* tab.

To lock an ADOM from the Device Manager tab:

1. Right-click on the ADOM name in the tree menu and select *Lock* from the pop-up menu.
   The ADOM will now be locked, allowing you to make changes to it, and preventing other administrators from making any changes, unless lock override is enabled.

To lock an ADOM from the Policies and Objects tab:

1. Select the specific ADOM that you are locking from the drop-down list in the toolbar, or select *Global*.
2. Select the lock icon next to the drop-down list 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, unless lock override is enabled.

To unlock the ADOM from the Policies and Objects tab:

1. Select the specific ADOM that you have locked from the drop-down list in the toolbar.
2. Select the locked icon next to the drop-down list to unlock the selected ADOM.
   The ADOM will now be unlocked, allowing you or another administrator to lock the ADOM and make further changes.

Workflow mode

Workflow mode is a new global mode to define approval or notification workflow when creating and installing policy changes. Workflow mode is enabled via the CLI only and requires workspace to also be enabled. When workflow mode is enabled, the administrator will have a new option in the admin page to approve/reject workflow requests.

This mode introduces three new permissions for Super_Admin administrative users:

- Self-approval: The user has rights to approve or deny changes without approvals. The user cannot approve the changes of others without the Approval right.
- Approval: The user has rights to rights to approve or deny the changes made by other users. The user cannot approve their own changes without the Self-approval right. When workflow mode is enabled, all administrators with the Approval right will receive notifications by default.
- Change Notification: The user is notified via email of all changes made on the FortiManager.

For administrators with the appropriate permissions, they will be able to approve or reject any pending requests. When viewing the session list, they can choose any sessions that are pending and click the approve/reject buttons. They can add a note to the approval/rejection response. The system will send a notification to the administrator that submitted the session. If the session was approved, no further action is required. If the session was rejected, the administrator will need to log on and repair their changes. Once they create a session, the administrator will make their repair on top of the last session changes.

Email notifications will be generated for the following situations:

- A new change is pending approval. The email will contain a summary of the changes.
- A change is approved.
- A change is denied.

When you want to start a workflow, go to the *Policy & Objects* tab and select the *Start Session* button. This will lock the ADOM, generate a revision, and allow you to make changes. When you are done making changes, select the *Submit* button. Once the session is submitted, the lock is released and other administrators may initiate a session.

The session list allows user to view any pending requests for approval or active sessions. The session list displays details of each session and allows you to browse the changes performed for the selected session.

To enable workflow mode and disable concurrent ADOM access type the following CLI command lines:

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

When enabling workflow mode, your session will end and you will be required to log back into your FortiManager.

Workflow Mode

Workflow mode is a new global mode to define approval or notification workflow when creating and installing policy or object changes. Workflow mode is enabled via the CLI only. When workflow mode is enabled, an administrator with the appropriate workflow permissions will be able to approve or reject workflow sessions before they are implemented to the database.

When you want to start a workflow, go to the *Policy & Objects* tab, select the ADOM from the drop-down list, lock the ADOM, and select the *Create New Session* button. You can then proceed to make changes to policies and objects. When you are done making changes, select the *Save* button and then the *Submit* button. Once the session is submitted, the lock is released and other administrators may initiate a session.

The session list allows user to view any pending requests for approval or active sessions. The session list displays details of each session and allows you to browse the changes performed for the selected session.

Enable or disable workflow mode

You can enable or disable workflow mode from the CLI only.

To enable or disable workflow mode:

1. Select the *System Settings* tab in the navigation pane.
2. Go to *System Settings* > *Dashboard*.
3. In the CLI Console widget type the following CLI command lines:

```
config system global
   set workspace-mode {workflow | disable}
end
```

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

When `workspace-mode` is `workflow`, the *Device Manager* tab and *Policy & Objects* tab are read-only. You must lock the ADOM to create a new workflow session.

Optionally, you can select to enable or disable ADOM lock override. When this feature is enabled, an administrator can select to unlock an ADOM that is locked by another administrator.

To enable or disable ADOM lock override:

1. Select the *System Settings* tab in the navigation pane.
2. Go to *System Settings* > *Dashboard*.
3. In the CLI Console widget type the following CLI command lines:

```
config system global
   set lock-prempt {enable | disable}
end
```

Workflow sessions

When you want to start a workflow, go to the *Policy & Objects* tab, select the ADOM from the drop-down list, lock the ADOM, and select the *Create New Session* button in the *Session List* dialog box. Type a name for the session and select *OK*. You can then proceed to make changes to policy packages and objects. When you are done making changes, select the *Save* button and then the *Submit* button in the toolbar. In the *Submit for Approval* dialog box, type a comment and the notification email. Once the session is submitted, the lock is released and other administrators may initiate a session.

For administrators with the appropriate permissions, they will be able to approve or reject any pending requests. When viewing the session list, they can choose any sessions that are pending and click the approve/reject buttons. They can add a note to the approval/rejection response. The system will send a notification to the administrator that submitted the session. If the session was approved, no further action is required. If the session was rejected, the administrator will need to log on and repair their changes. Once they create a session, the administrator will make their repair on top of the last session changes.

To start a workflow session:

1. Select the *Policy & Objects* tab in the navigation pane.
2. Select the ADOM from the drop-down list.
3. Select *Lock ADOM* in the toolbar. The lock icon changes to a locked state and the *Session List* window is displayed.
4. Select the *Create New Session* button, type a name for new session, type optional comments, and select *OK* to start the session.
5. Make the required changes to *Policy Package* and *Objects* and select *Sessions* > *Submit* in the toolbar to submit changes for approval. The *Submit for Approval* dialog box is displayed.

   Enter the following:

Comments	Type a comment for the session.
Attach configuration change details	Select to attach configuration change details to the email.

6. Select *OK* to send submit the session for approval.

   The session is submitted for approval, an email is sent to the approver, and the ADOM is returned to an unlocked state. An ADOM revision is created for the workflow session.

To approve, reject, or repair a workflow session:

1. Select the *Policy & Objects* tab in the navigation pane.
2. Select the ADOM from the drop-down list.
3. Select *Lock ADOM* in the toolbar. The lock icon changes to a locked state and the Session List window is displayed. Alternatively, select *Sessions* > *Session List* from the toolbar.

   The following information is displayed:

ID	The session identifier.

Status	The session status. One of the following: • *Waiting Approval*: The session is waiting to be reviewed and approved. • *Approved*: The workflow session was approved by the approver. • *Rejected*: The workflow session was rejected by the approver. • *Repaired*: The rejected workflow session was repaired. When a rejected session is repaired, a new session ID is created for this repaired session.
Name	The user defined name to identify the session.
User	The administrator name who created the session.
Date Submitted	The date and time that the session was submitted for approval.
Comments	Select a policy in the list to view or add comments to the session. The comments box displays comments from the session creator. The session approver can add comments.
Create New Session	Select to create a new workflow session.
Continue Without Session	Select to continue without starting a new session. When a new session is not started, all policy and objects are read-only.

Right-clicking on a session in the list opens a pop-up menu with the following options:

Approve	Select *Approve* when the session status is *Waiting Approval*.
Reject	Select *Reject* when the session status is *Waiting Approval*. A rejected session must be repaired before the next session in the list can be approved.
Repair	Select *Repair* when the session status is *Rejected*. A repaired session results in a new session being created for the repair. This session is added after the last session in the list.
View Diff	Select *View Diff* to view the difference between the two revisions. You can select to download the revision in a CSV file to your management computer.

4. Select to *Approve*, *Reject*, *Repair*, or *View Diff*.

A session that is rejected must be fixed before the next session can be approved.

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 permissions, managing and updating firmware for the device and configuring logging and access to the *FortiGuard Update Service* for updates.

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

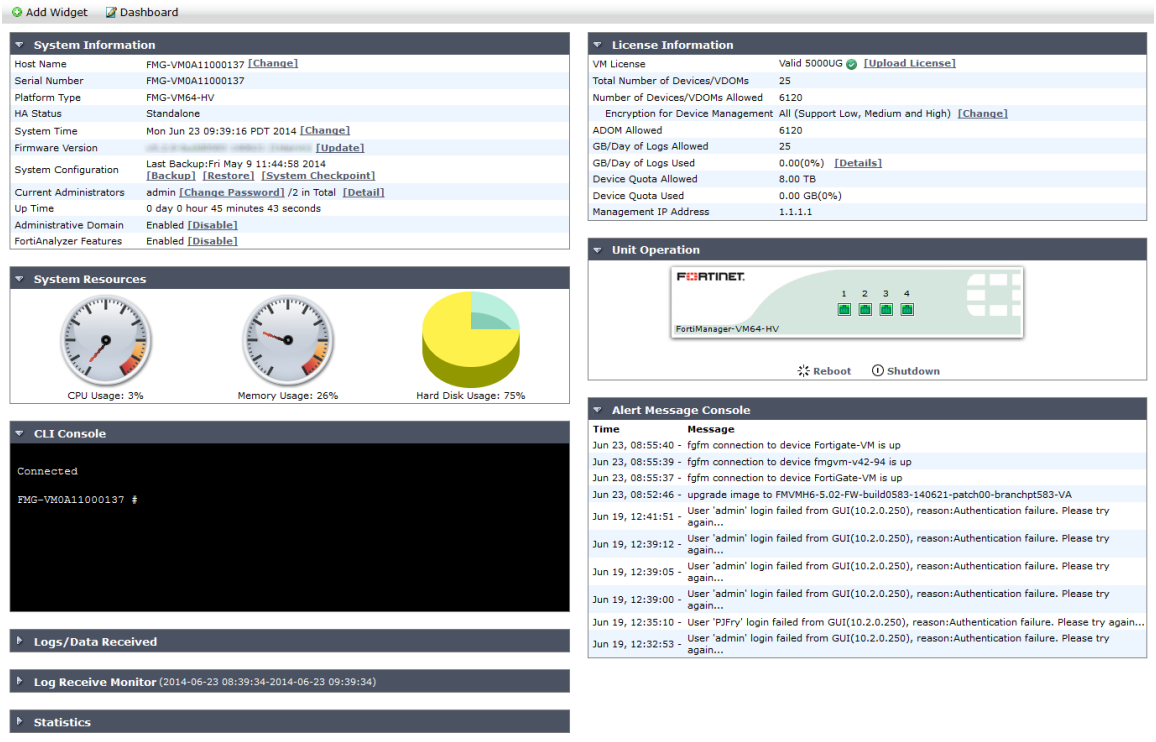
Dashboard	The Dashboard page displays widgets that provide performance and status information and enable you to configure basic system settings.
All ADOMs	The All ADOMS page is only available when ADOMs are enabled. It lists all of the ADOMs, version, devices, VPN management, number of policy packages and alert device information. On this page you can create, edit, delete and upgrade ADOMs. You can also view the alert device details.
RAID management	The RAID Management page displays information about the status of RAID, as well as what RAID level has been selected and how much disk space is currently consumed.
Network	The Network page provides routing and interface management options. It also provides access to diagnostic tools, such as ping, and a detailed listing of all currently configured interfaces.
High availability	The HA page allows you to configure operation mode and cluster settings.
Admin	Select this menu to configure administrator user accounts, as well as configure global administrative settings for the FortiManager unit. • Administrator • Profile • Workflow Approval • Remote authentication server • Administrator settings • Configure two-factor authentication for administrator log on
Certificates	The Certificates section allows you to configure local and CA certificates, and Certificate revocation lists (CRLs).
Event log	View log messages that are stored in memory or on the internal hard disk. On this page you can view historical or real-time logs and download event logs.
Task monitor	The Task Monitor page allows you to view the status of the tasks that you have performed.

Advanced	Select to configure mail server settings, remote output, Simple Network Management Protocol (SNMP), meta field data and other advanced settings. • SNMP • Mail server • Syslog server • Meta fields • Device log settings • File management • Advanced settings • Portal users

Dashboard

When you select the *System Settings* tab, it automatically opens at the *System Settings* > *Dashboard* page.

The *Dashboard* displays widgets that provide performance and status information and enable you to configure basic system settings. The dashboard also contains a CLI widget that allows you to use the command line through the GUI. All of the widgets appear on a single dashboard, which can be customized as desired.



The following widgets are available:

System Information	Displays basic information about the FortiManager system, such as up time and firmware version. You can also enable or disable Administrative Domains and FortiAnalyzer features. For more information, see System Information widget on page 48. From this widget you can manually update the FortiManager firmware to a different release. For more information, see Firmware images on page 325.
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 55. From this widget you can manually upload a license for FortiManager VM systems.
Unit Operation	Displays status and connection information for the ports of the FortiManager unit. It also enables you to shutdown and restart the FortiManager unit or reformat a hard disk. For more information, see Unit Operation widget on page 57.
System Resources	Displays the real-time and historical usage status of the CPU, memory and hard disk. For more information, see System Resources widget on page 54.
Alert Message Console	Displays log-based alert messages for both the FortiManager unit itself and connected devices. For more information, see Alert Messages Console widget on page 57.
CLI Console	Opens a terminal window that enables you to configure the FortiManager unit using CLI commands directly from the GUI. This widget is hidden by default. For more information, see CLI Console widget on page 58.
Log Receive Monitor	Displays a real-time monitor of logs received. You can select to view data per device or per log type. For more information, see Log Receive Monitor widget on page 59. The *Log Receive Monitor* widget is available when *FortiAnalyzer Features* is enabled.
Logs/Data Received	Displays real-time or historical statistics of logs and data received. For more information, see Logs/Data Received widget on page 59. The *Log/Data Received* widget is available when *FortiAnalyzer Features* is enabled.
Statistics	Displays statistics for logs and reports. For more information, see Statistics widget on page 60. The *Statistics* widget is available when *FortiAnalyzer Features* is enabled.
Insert Rate vs Receive Rate	Displays the log insert and receive rates. For more information, see Insert Rate vs Receive Rate widget on page 61. The *Insert Rate vs Receive Rate* widget is available when *FortiAnalyzer Features* is enabled.

Log Insert Lag Time	Displays the log insert lag time, in seconds. For more information, see Log Insert Lag Time widget on page 61. The *Log Insert Lag Time* widget is available when *FortiAnalyzer Features* is enabled.

Customizing the dashboard

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

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 remove a widget, select the *Close* icon.

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.

The following options are available:

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 in the *Alert Message Console* widget.
Edit	Select to change settings for the widget. This option appears only in the *System Resources*, *Alert Message Console*, *Logs/Data Received*, and *Log Receive Monitor* widgets.
Detach	Detach the CLI Console widget from the dashboard and open it in a separate window. This option appears only in the *CLI Console* widget.
Reset	Select to reset the information shown in the widget. This option appears only in the *Statistics* 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 System Information widget on page 48, which displays the current status of the FortiManager unit and enables you to configure basic system settings.

The information displayed in the *System Information* widget is dependent on the FortiManager models and device settings. The following information is available on this widget:

Host Name	The identifying name assigned to this FortiManager unit. Select *[Change]* to change the host name. For more information, see Changing the host name on page 49.
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 327.
System Time	The current time on the FortiManager internal clock. Select *[Change]* to change system time settings. For more information, see Configuring the system time on page 50.
Firmware Version	The version number and build number of the firmware installed on the FortiManager unit. To update the firmware, you must download the latest version from the Customer Service & Support website at https://support.fortinet.com. 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 50.
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 51. • Select *[Restore]* to restore the configuration from a backup file; see Restoring the configuration on page 52. • Select *[System Checkpoint]* to revert the system to a prior saved configuration; see Creating a system checkpoint on page 53.

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 *[Detail]* to view the session details for all currently logged in administrators. See Monitoring administrator sessions on page 74 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. Select *[Enable/Disable]* to change the Administrative Domain state. SeeEnabling and disabling the ADOM feature on page 32.
Global Database Version	Displays the current Global Database version. Select *[Change]* to change the global database version.
Offline Mode	Displays whether Offline Mode is enabled. To enable or disable Offline Mode, go to *System Settings* > *Advanced* > *Advanced Settings*.
FortiAnalyzer Features	Displays whether FortiAnalyzer features are enabled. Select *[Enable/Disable]* to change the FortiAnalyzer features state. *FortiAnalyzer Features* are not available on the FAZ-100C.

The following options are available:

Refresh	Select the refresh icon in the title bar to refresh the information displayed.
Close	Select the close icon in the title bar to remove the widget from the dashboard.

Changing the host name

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

- It appears in the *System Information* widget on the *Dashboard*. For more information about the *System Information* widget, see System Information widget on page 48.
- It is used in the command prompt of the CLI.
- It is used as the SNMP system name. For information about SNMP, see SNMP on page 107.

The *System Information* widget and the `get system status` CLI command will display the full host name. However, if the host name is longer than 16 characters, the CLI and other places display the host name in a truncated form ending with a tilde (~) to indicate that additional characters exist, but are not displayed. For example, if the host name is FortiManager1234567890, the CLI prompt would be `FortiManager123456~#`.

To change the host name:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, next to the *Host Name* field, select *[Change]*.
3. In the *Host Name* box, type a new host name.

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

4. Select *OK*.

Configuring the system time

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

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

To configure the date and time:

1. Go to *System Settings* > *General* > *Dashboard*.
2. In the *System Information* widget, in the *System Time* field, select *Change*. The *Change System Time Settings* dialog box opens.
3. Configure the following settings to either manually configure the system time, or to automatically synchronize the FortiManager unit's clock with an NTP server:

System Time	The date and time according to the FortiManager unit's clock at the time that this tab was loaded, or when you last selected the *Refresh* button.
Time Zone	Select the time zone in which the FortiManager unit is located and whether or not the system automatically adjusts for daylight savings time.
Set Time	Select this option to manually set the date and time of the FortiManager 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 FortiManager unit's clock with an NTP server, then configure the *Syn Interval* and *Server* fields before you select *OK*.
Sync Interval	Type how often in minutes the FortiManager unit should synchronize its time with the NTP server. For example, entering 1440 causes the FortiManager unit to synchronize its time once a day.
Server	Type 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. Select the add icon to add an NTP server. Select the delete icon to delete an NTP server.

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.

For information about upgrading your FortiManager device, see the FortiManager Release Notes or contact Fortinet Customer Service & Support.

Back up the configuration and database before changing the firmware of your FortiManager unit. Changing the firmware to an older or incompatible version may reset the configuration and database to the default values for that firmware version, resulting in data loss. For information on backing up the configuration, see Backing up the system on page 51.

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

To manually update the FortiManager firmware:

1. Download the firmware (the `.out` file) from the Customer Service & Support website, https://support.fortinet.com/.
2. Go to *System Settings* > *Dashboard*.
3. In the *System Information* widget, 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 website, 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 FortiManager unit installs the firmware and restarts.
   If you changed the firmware to an earlier version whose configuration is not compatible, you may need to do first-time setup again. For instructions, see the *FortiManager QuickStart Guide* for your unit.
8. Update the vulnerability management engine and definitions.

Installing firmware replaces the current network vulnerability management engine with the version included with the firmware release that you are installing. After you install the new firmware, make sure that your vulnerability definitions are up-to-date. For more information, see FortiGuard Management on page 307.

The FortiManager firmware can also be updated through the FDN. For more information, see Firmware images on page 325.

Backing up the system

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

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

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

To back up the FortiManager configuration:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, under *System Configuration*, select *[Backup]*. The *Backup* dialog box opens.
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	Type the password again. The passwords must match.

4. If you want to encrypt the backup file, select the *Encryption* check box, then type 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.

The restore operation will temporarily disable the communication channel between FortiManager and all managed devices. This is a safety measure, in case any devices are being managed by another FortiManager. To re-enable the communication, please go to *System Settings* >*Advanced* >*Advanced Settings* and disable *Offline Mode*.

To restore the FortiManager configuration:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, under *System Configuration*, select *[Restore]*. The *Restore* dialog box appears.
3. Configure the following settings then select *OK*.

From Local	Select *Browse* to find the configuration backup file you want to restore.
Password	Type the encryption password, if applicable. The password can be a maximum of 15 characters.

Overwrite current IP, routing and HA settings	Select the check box to overwrite the current IP, routing and HA settings.
Restore in Offline Mode	Informational check box. Hover over the help icon for more information.

Creating a system checkpoint

You can create a system checkpoint backup to capture a specific configuration. This backup provides a history where the FortiManager and FortiGate units are completely in sync. Should there be a major failure, you can completely revert the FortiManager to when it was in working order. These are, in essence, snapshots of your FortiManager managed network system.

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

A system checkpoint backup includes the system configuration of the FortiManager unit.

Please note the following:

- The system checkpoint does not include the FortiGate settings.
- For policy package specific settings, after reverting to a checkpoint, you need to re-install policy packages to update FortiGate policy and related configuration.
- For non-policy package settings, after reving to a checkpoint, you must trigger FortiGate to auto-update and overwrite the checkpoint reverted configuration. Alternatively, you can disable the auto update function in System Settings and re-install the checkpoint reverted configuration to FortiGate.

To create a system checkpoint:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, under *System Configuration*, select *[System Checkpoint]*. The *System Checkpoint* table opens.
3. Select *Create New*. The *Create New System Checkpoint* dialog box opens.
4. In the *Comments* box, type a description, up to 63 characters, for the reason or state of the backup.
5. Select *OK*. The system checkpoint task will be run and the checkpoint will be created.

To revert to a system checkpoint:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, under *System Configuration*, select *[System Checkpoint]*. The *System Checkpoint* table opens.
3. Select the system checkpoint in the table and select the revert icon.
4. A confirmation dialog box will open. Select *OK* to continue.

When reverting to a system checkpoint, the FortiManager will reboot.

To delete a system checkpoint:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, under *System Configuration*, select *[System Checkpoint]*. The *System Checkpoint* table opens.
3. Select the system checkpoint in the table and select the *Delete* in the toolbar.
4. A confirmation dialog box will open. Select *OK* to continue.

Enable or disable FortiAnalyzer features

The FortiAnalyzer feature set can enabled or disabled via the CLI using the following command:

```
config system global
   set faz-status {enable | disable}
end
```

You can also enable or disable these features in the FortiManager GUI. The FortiAnalyzer feature set includes the following modules: FortiView, Event Management, and Reports. Other menu items are FortiAnalyzer related including *Device Log Settings* and *File Management*.

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

To enable the FortiAnalyzer feature set

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, select *[Enable]* beside *FortiAnalyzer Features*. A confirmation dialog box is displayed.
3. Select *OK* to continue. Your FortiManager will reboot to apply the change.

To disable the FortiAnalyzer feature set

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, select *[Disable]* beside *FortiAnalyzer Features*. A confirmation dialog box is displayed.
3. Select *OK* to continue. Your FortiManager will reboot to apply the change.

System Resources widget

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

The following information is displayed on this widget:

CPU Usage	The current CPU utilization. The GUI displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the GUI) is excluded. The average CPU usage can be shown, as well as the usage for each CPU core.

Memory Usage	The current memory utilization. The GUI displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the GUI) 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.

The following options are available:

Edit	Select the edit icon in the title bar to edit widget settings including multi-core CPU display, view type, and refresh interval.
Refresh	Select the refresh icon in the title bar to refresh the information displayed.
Close	Select the close icon in the title bar to remove the widget from the dashboard.

Change the system resource widget display settings:

1. Go to *System Settings* > *Dashboard*.
2. In the System Resources widget, move the pointer over the title bar and select the *Edit* icon.
   The *Edit System Resources Settings* dialog box appears.
3. Configure the following settings:

Multi-core CPU Display	To view the resource information for all the cores as an average, from *Multi-core CPU Display*, select *Average*, or, to view individual information for each core, select *Each Core* (the default value).
View Type	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*.
Refresh Interval	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 data sheet for more information on your specific device.

The following information is displayed in this widget:

VM License	VM license information and status. Select *[Upload License]* to upload a new VM license file. This field is only visible for FortiManager VM.
Total Number of Devices/VDOMs	The total number of devices and VDOMs configured on this FortiManager.
Encryption for Device Management	The encryption mode for device management. Select *[Change]* to change the encryption mode. Select one of the following: • All (Support Low, Medium, and High) • Medium (support Medium and High) • High (Support High only)
ADOM Allowed	The number of ADOMs allowed to be configured on this FortiManager. The ADOM maximum value is dependent on the FortiManager model.
GB/Day of Logs Allowed	The GB per day of logs allowed for this FortiManager. This field is only visible when *FortiAnalyzer Features* is enabled.
GB/Day of Logs Used	The GB per day of logs used for this FortiManager. Select *[Details/Hide]* to view the GB per day of logs used for the previous 6 days. This field is only visible when *FortiAnalyzer Features* is enabled.
Device Quota Allowed	The device quota allowed for this FortiManager. This field is only visible when *FortiAnalyzer Features* is enabled.
Device Quota Used	The device quota used for this FortiManager. This field is only visible when *FortiAnalyzer Features* is enabled.
Management IP Address	The FortiManager VM management IP address associated with the FortiManager VM license. This field is only visible for FortiManager VM. For more information on changing the management IP address, see the *FortiManager VM Install Guide*.

The following options are available:

Refresh	Select the refresh icon in the title bar to refresh the information displayed.
Close	Select the close icon in the title bar to remove the widget from the dashboard.

To change the encryption mode:

1. In the *License Information* widget, select *Change* in the *Encryption for Device Management* field. The *Change Encryption Mode* dialog box opens.
2. Select *All*, *Medium*, or *High* for the encryption mode.
3. Select OK to apply the change.

To view the details of the GB/Day of logs used:

Select *Details* in the *GB/Day of Logs Used* field. The field will expand to show the number of GB used per day for today and the past 6 days.

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.

The following information is displayed in this 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 move the pointer 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.

The following options are available:

Refresh	Select the refresh icon in the title bar to refresh the information displayed.
Close	Select the close icon in the title bar to remove the widget from the dashboard.

Alert Messages Console widget

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

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

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

The following options are available:

More Alerts	For a complete list of unacknowledged alert messages, select the *More Alerts* icon in the widget's title bar.
Edit	Select the edit icon in the title bar to edit widget settings including the number of entries and refresh interval.
Refresh	Select the refresh icon in the title bar to refresh the information displayed.
Close	Select the close icon in the title bar to remove the widget from the dashboard.

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

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 type command lines through the GUI, without making a separate Telnet, SSH, or local console connection to access the CLI.

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

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 GUI. 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 `FortiManager-800B #`, contains the host name of the FortiManager unit. To change the host name, see Changing the host name on page 49

The following options are available:

Detach	The CLI Console widget can be opened in a new window by selecting the detach icon in the widget's title bar.
Refresh	Select the refresh icon in the title bar to refresh the information displayed.

For information on available CLI commands, see the *FortiManager* CLI Reference available in the Fortinet Document Library webpage.

Log Receive Monitor widget

The Log Receive Monitor widget displays the rate at which logs are received over time. You can select to display log data either by log type or per device.

This widget is available in the GUI when *FortiAnalyzer Features* is enabled. For more information, see Enable or disable FortiAnalyzer features on page 54.

The following options are available:

Edit	Select the edit icon in the title bar to edit widget settings including the type, number of entries, time period, and refresh interval.
Refresh	Select the refresh icon in the title bar to refresh the information displayed.
Close	Select the close icon in the title bar to remove the widget from the dashboard.

To configure settings for the widget, select the edit icon from the title bar to view the *Edit Log Receive Monitor Settings* dialog box.

Configure the following settings:

Type	Select either: • *Log Type*: Display the type of logs that are received from all registered devices and separates them into categories. The categories include *Event, Email Filter, Mail Statistics, Traffic, Web Filter*, and *Other*. • *Device*: Display the logs that received by each registered device and separates the devices into the top number of devices.
Number of Entries	Select the number of either log types or devices in the widget's graph, depending on your selection in the *Type* field.
Time Period	Select one of the following time ranges over which to monitor the rate at which log messages are received: *Hour*, *Day*, or *Week*.
Refresh Interval	To automatically refresh the widget at intervals, type a number between 10 and 240 seconds. To disable the refresh interval feature, type `0`.

Logs/Data Received widget

The *Logs/Data Received* widget displays the rate over time of the logs and data, such as Traffic, Web Filter, and Event logs, received by the FortiManager unit.

This widget is available in the GUI when *FortiAnalyzer Features* is enabled. For more information, see Enable or disable FortiAnalyzer features on page 54.

The widget displays the following information:

Logs Received	Number of logs received per second.
Data Received	Volume of data received.

The following options are available:

Edit	Select the edit icon in the title bar to edit widget settings including the view type and refresh interval.
Refresh	Select the refresh icon in the title bar to refresh the information displayed.
Close	Select the close icon in the title bar to remove the widget from the dashboard.

To configure settings for the widget, select the edit icon from the title bar to view the *Edit Logs/Data Received Settings* dialog box.

Configure the following settings:

View Type	Select *Real Time* to view current information about system resources. Select *Historical* to view historical information.
Time Period	Select one of the following to set the time period displayed: *Last 10 Minutes*, *Last 1 Hour,* or *Last 24 Hours*. This option is only available when the view is set to *Historical*.
Refresh Interval	To automatically refresh the widget at intervals, type a number between 10 and 240 seconds. To disable the refresh interval feature, type `0`.

Statistics widget

The *Statistics* widget displays the numbers of sessions, volume of log files, and number of reports handled by the FortiManager unit.

This widget is available in the GUI when *FortiAnalyzer Features* is enabled. For more information, see Enable or disable FortiAnalyzer features on page 54.

The widget displays the following information:

Logs	The number of new log files received from a number of devices since the statistics were last reset.
Log Volume	The average log file volume received per day over the past seven days.
Reports	The number of reports generated for a number of devices.

The following options are available:

Reset	Select the reset icon in the title bar to reset statistics.
Refresh	Select the refresh icon in the title bar to refresh the information displayed.
Close	Select the close icon in the title bar to remove the widget from the dashboard.

Insert Rate vs Receive Rate widget

The *Insert Rate vs Receive Rate* widget displays the log insert and log receive rates in a line graph.

- Log receive rate: how many logs are being received.
- Log insert rate: how many logs are being actively inserted into the datebase.

If the log insert rate is higher than the log receive rate, then the database is rebuilding. The lag is the number of logs that are waiting to be inserted.

Hover the cursor over a point on the graph to see the exact number of logs that were received and inserted and a specific time.

Select the edit icon in the widget toolbar to adjust the time interval shown on the graph (last 1 hour, 8 hours, or 24 hours) and the refresh interval (60 - 240 seconds, 0 to disable) of the widget.

Log Insert Lag Time widget

The *Log Insert Lag Time* widget shows the how many seconds the database is behind in processing the logs.

Select the edit icon in the widget toolbar to adjust the time interval shown on the graph (last 1 hour, 8 hours, or 24 hours) and the refresh interval (60 - 240 seconds, 0 to disable) of the widget.

All ADOMs

To view a listing of all the ADOMs and to create new ADOMs, go to *System Settings* > *All ADOMs*. Default ADOMs including FortiAnalyzer, FortiCache, FortiCarrier, FortiClient, FortiMail, FortiSandbox, FortiWeb, Syslog, root, and Global Database.

The following information is available:

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 following options are available. Right-clicking on an ADOM in the list opens a menu with the additional options:

Create New	Select to create a new ADOM. For information on creating a new ADOM, see Adding an ADOM on page 36
Delete	Select to delete the ADOM. This option is greyed out for default ADOMs which cannot be deleted. An ADOM which contains user(s), device(s) and/or group(s) cannot be deleted. An ADOM which is locked by another administrator also cannot be deleted.
Edit	Select to edit the ADOM. The following ADOMs cannot be edited: FortiAnalyzer, FortiCache, FortiClient, FortiMail, FortiManager, FortiSandbox, FortiWeb, and Syslog.
Upgrade	Select to upgrade the ADOM. This option is available when upgrading a v4.3 ADOM to v5.0 or a v5.0 ADOM to v5.2.
Select All	Select to select all ADOMs. Default ADOMs including FortiAnalyzer, FortiCache, FortiCarrier, FortiClient, FortiMail, FortiSandbox, FortiWeb, Syslog, root, and Global Database will not be selected.

The ADOMs in the list can also be edited and deleted as required. See Managing ADOMs on page 35 for more information.

The ADOM version can also be upgraded. See Upgrading an ADOM on page 37 for more information.

An ADOM can only be upgraded after all the devices within the ADOM have been upgraded. See ADOM versions on page 34 for more information.

Change the global database version:

1. Go to *System Settings* > *All ADOMs*.
2. Right-click Global Database and select *Edit* in the menu.
   The *Edit ADOM* dialog box is displayed.
3. Select the version from the drop-down list.
4. Select *OK* to save the setting.
5. A confirmation dialog box will be displayed. Select *OK* to continue.

Changing the global database version will reset the global database.

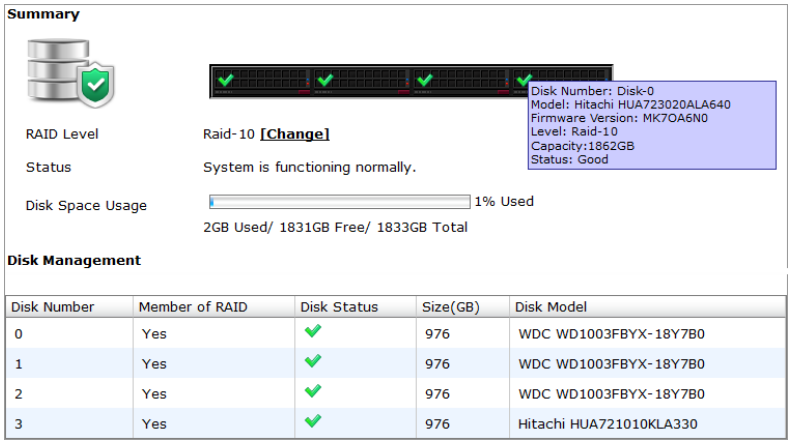
RAID management

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

You can view the status of the RAID array from the RAID Management page found at *System Settings* > *RAID Management*. This page displays the status of each disk in the RAID array, including the system's RAID level. This widget also displays how much disk space is being used.

The *Alert Message Console* widget, located in *System Settings* > *Dashboard*, provides detailed information about RAID array failures. For more information see Alert Messages Console widget on page 57.

If you need to remove a disk from the FortiManager unit, you may be able to hot swap it. Hot swapping means replacing a hard disk while the device 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 65.



The following information is displayed in this page:

Summary	Hover the mouse cursor over a disk to view the disk number, model, firmware version, level, capacity, and status.
RAID Level	The RAID level. Select *[Change]* to change the RAID level. Select the RAID level from the drop-down list and select *OK*. If RAID settings are changed, all data will be deleted.
Status	The RAID status is displayed.
Disk Space Usage	The disk space usage is displayed as a percentage. The amount of space used, free, and total is also displayed.
Disk Management	The table lists the disk number, member of RAID, disk status, disk size, and disk model.

To configure the RAID level:

1. Go to *System Settings* > *RAID Management*.
2. Select *Change* in the *RAID Level* field. The *RAID Settings* dialog box opens.

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

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

Supported RAID levels

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

Linear RAID

A Linear RAID array combines all hard disks into one large virtual disk. The total space available in this option is the capacity of all disks used. There is very little performance change when using this RAID format. If any of the drives fails, the entire set of drives is unusable until the faulty drive is replaced. All data will be lost.

RAID 0

A RAID 0 array is also referred to as striping. The FortiManager unit writes information evenly across all hard disks. The total space available is that of all the disks in the RAID array. There is no redundancy available. If any single drive fails, the data on that drive cannot be recovered. This RAID level is beneficial because it provides better performance, since the FortiManager unit can distribute disk writing across multiple disks.

RAID 1

A RAID 1 array is also referred to as mirroring. The FortiManager unit writes information to one hard disk, and writes a copy (a mirror image) of all information to all other hard disks. The total disk space available is that of only one hard disk, as the others are solely used for mirroring. This provides redundant data storage with no single point of failure. Should any of the hard disks fail, there are several backup hard disks available.

RAID 1 +Spare

A RAID 1 with hot spare array uses one of the hard disks as a hot spare (a stand-by disk for the RAID). If a hard disk fails, within a minute of the failure, the hot spare is substituted for the failed drive, integrating it into the RAID array, and rebuilding the RAID's data. When you replace the failed hard disk, the new hard disk is used as the new hot spare. The total disk space available is the total number of disks minus two.

RAID 5

A RAID 5 array employs striping with a parity check. Similar to RAID 0, the FortiManager unit writes information evenly across all drives but additional parity blocks are written on the same stripes. The parity block is staggered for each stripe. The total disk space is the total number of disks in the array, minus one disk for parity storage. For example, with four hard disks, the total capacity available is actually the total for three hard disks. RAID 5 performance is typically better with reading than with writing, although performance is degraded when one disk has failed or is missing. With RAID 5, one disk can fail without the loss of data. If a drive fails, it can be replaced and the FortiManager unit will restore the data on the new disk by using reference information from the parity volume.

RAID 5 +Spare

A RAID 5 with hot spare array uses one of the hard disks as a hot spare (a stand-by disk for the RAID). If a hard disk fails, within a minute of the failure, the hot spare is substituted for the failed drive, integrating it into the RAID array, and rebuilding the RAID's data. When you replace the failed hard disk, the new hard disk is used as the new hot spare. The total disk space available is the total number of disks minus two.

RAID 6

A RAID 6 array is the same as a RAID 5 array with an additional parity block. It uses block-level striping with two parity blocks distributed across all member disks.

RAID 6 +Spare

A RAID 6 with hot spare array is the same as a RAID 5 with hot spare array with an additional parity block.

RAID 10

RAID 10 (or 1+0), includes nested RAID levels 1 and 0, or a stripe (RAID 0) of mirrors (RAID 1). The total disk space available is the total number of disks in the array (a minimum of 4) divided by 2, for example:

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.

RAID 50

RAID 50 (or 5+0) includes nested RAID levels 5 and 0, or a stripe (RAID 0) and stripe with parity (RAID 5). The total disk space available is the total number of disks minus the number of RAID 5 sub-arrays. RAID 50 provides increased performance and also ensures no data loss for the same reasons as RAID 5. One drive in each RAID 5 array can fail without the loss of data.

RAID 50 is only available on models with 9 or more disks. By default, two groups are used unless otherwise configured via the CLI. Use the `diagnose system raid status` CLI command to view your current RAID level, status, size, groups, and hard disk drive information.

RAID 60

A RAID 60 (6+0) array combines the straight, block-level striping of RAID 0 with the distributed double parity of RAID 6. It requires at least eight disks.

Hot swapping hard disks

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

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

To identify which hard disk failed, read the relevant log message in the *Alert Message Console* widget (see Alert Messages Console widget on page 57).

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 page 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.

Adding new disks

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

Fortinet recommends that you use the same disks as those supplied by Fortinet. Disks of other brands will not be supported by Fortinet. For information on purchasing extra hard disks, contact your Fortinet reseller.

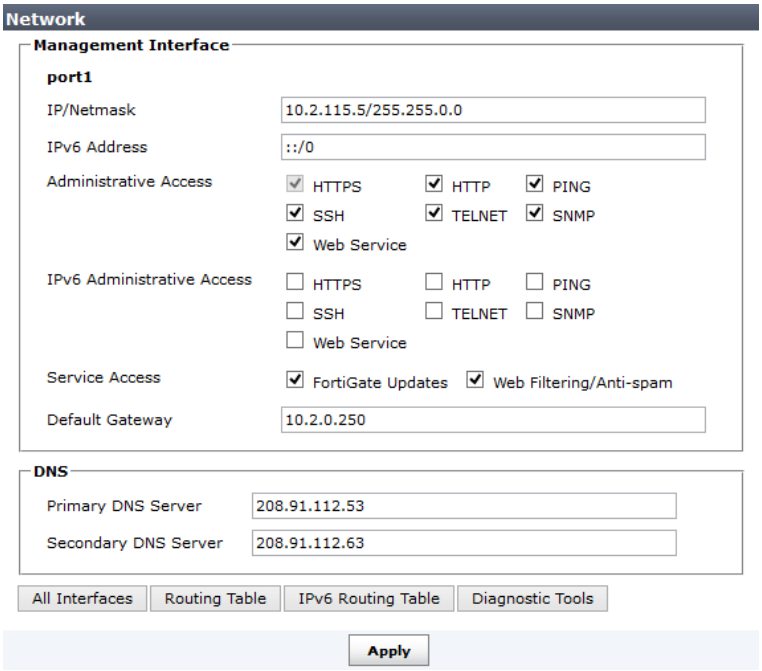
To add more hard disks:

1. Obtain the same disks as those supplied by Fortinet.
2. Back up the log data on the FortiManager unit.
   You can also migrate the data to another FortiManager unit if you have one. Data migration reduces system down time and risk of data loss. For information on data backup, see Backing up the system on page 51.
3. Install the disks on the FortiManager unit. If your unit supports hot swapping, you can do so while the unit is running.
4. Configure the RAID level.
   If you have backed up the log data, restore the data. For more information, see Restoring the configuration on page 52.

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* > *Network*. The Network screen is displayed.



The following information is displayed:

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 Admin-istrative 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 /antispam.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	Type the primary DNS server IP address.
	Secondary DNS Server	Type the secondary DNS server IP address.

The following options are available:

All Interfaces	Click to open the network interface list. See Viewing the network interface list on page 68.
Routing Table	Click to open the routing table. See Configuring static routes on page 70.
IPv6 Routing Table	Click to open the IPv6 routing table. See Configuring IPv6 static routes on page 70.
Diagnostic Tools	Select to run available diagnostic tools, including *Ping*, *Traceroute*, and *View logs*. See Diagnostic tools on page 71.
Apply	Select *Apply* to save the changes made in the *Management Interface* settings page.

Viewing the network interface list

To view the network interface list, select the *All Interfaces* button. Double-click an port to edit the interface.

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 69. 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, TELNET, SNMP, and Web Service.
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, an enabled icon appears in the column. If the interface is not enabled, a disabled icon appears in the column.

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

Edit	Select the interface in the table, right-click, and select *Edit* in the right-click menu to edit the entry. Alternatively, you can double-click the entry to open the *Edit Interface* page.
Delete	Select the interface in the table, right-click, and select *Delete* in the right-click menu to remove the entry. Select *OK* in the confirmation dialog box to complete the delete action.

Configuring network interfaces

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

The following settings are available.

Enable	Select to enable this interface. An enabled icon appears in the interface list to indicate the interface is accepting network traffic. When not selected, a disabled icon appears in the interface list to indicate the interface is down and not accepting network traffic.
Alias	Type an alias for the port to make it easily recognizable.
IP Address/Netmask	Type the IP address and netmask for the interface.
IPv6 Address	Type the IPv6 address for the interface.
Administrative Access	Select the services to allow on this interface. Any interface that is used to provide administration access to the FortiManager unit will require at least HTTPS or HTTP for 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	Type a brief description of the interface (optional).

Configuring static routes

Go to *System Settings* > *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.

The following information is displayed:

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.

The following options are available:

Create New	Select *Create New* to add a new route. Select the route number to edit the settings.
Edit	Select the checkbox next to the route number, right-click, and select *Edit* in the right-click menu to edit the entry. Alternatively, you can double-click the entry to open the *Edit Route* page.
Delete	Select the check box next to the route number and select *Delete* to remove the route from the table. Delete is also available in the right-click menu. Select *OK* in the confirmation dialog box to complete the delete action.

Add a static route

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

Configure the following settings, then select *OK* to create a new route:

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

Configuring IPv6 static routes

Go to *System Settings* > *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 is displayed:

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.

The following options are available:

Create New	Select *Create New* to add a new route. Select the route number to edit the settings.
Edit	Select the checkbox next to the route number, right-click, and select *Edit* in the right-click menu to edit the entry. Alternatively, you can double-click the entry to open the *Edit IPv6 Route* page.
Delete	Select the check box next to the route number and select *Delete* to remove the route from the table. Select *OK* in the confirmation dialog box to complete the delete action.

Add a IPv6 static route

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

Configure the following settings:

Destination IPv6 Prefix	Type the destination IPv6 prefix for this route.
Gateway	Type the IP address of the next hop router to which this route directs traffic.
Interface	Select the network interface that connects to the gateway.

Diagnostic tools

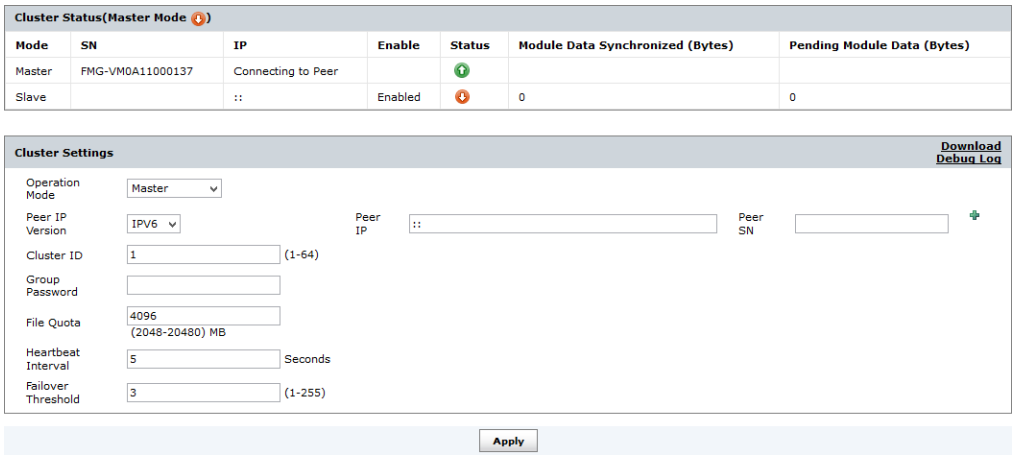
Go to *System Settings* > *Network* then select the *Diagnostic Tools* button. Here you can use the available diagnostic tools: *Ping* and *Traceroute*.

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* > *HA*. From here you can configure FortiManager units to start an HA cluster or you can change the HA configuration of the cluster.



Configure the following settings:

Cluster Status	Displays the cluster status include mode, serial number, IP address, enable, status, module data synchronized (bytes), and pending module data (bytes) for each cluster member.
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 Version	Select the IP version from the drop-down list.
Peer IP	Type 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. Select the add icon to add peers. Select the delete icon to remove a peer. For a backup unit you add the IP address of the primary unit.
Peer SN	Type 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 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 GUI browser window title changes to include the Group ID when FortiManager unit is operating in HA mode. Range: 0 to 64

Group Password	A password for the HA cluster. All members of the HA cluster must have the same group password. The maximum password length is 19 characters. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different password.
File Quota	Configure the maximum hard limit of hard disk space that the HA master can use to synchronize data to the slaves. Once the limit is reached, HA will reset itself instead of taking up more disk space. Range: 2048 to 20480 (MB) Default: 4096 (MB)
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. You cannot configure the heartbeat interval of the backup units. Range: 1 to 255 (seconds) Default: 5 (seconds)
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. 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. Range: 1 to 255 (seconds) Default: 3 (seconds0
Download Debug Log	Select to download the debug log. HA related activities are auto logged.

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

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

You can connect to the primary unit GUI to work with FortiManager. Because of configuration synchronization you can configure and work with the cluster in the same way as you would work with a standalone FortiManager unit.

When the cluster is operating, from the primary unit GUI 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 327.

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 75.
Profile	Select to set up access profiles for the administrative users. For more information, see Profile on page 86.
Workflow Approval	Select to create a new approval matrix or edit/delete an existing approval matrix. For more information, see Workflow Approval on page 90.
Remote Auth Server	Select to configure authentication server settings for administrative log in. For more information, see Remote authentication server on page 90.
Admin Settings	Select to configure connection options for the administrator including port number, language of the GUI and idle timeout. For more information, see Administrator settings on page 94.

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* > *Dashboard*. In the *System Information* widget, under *Current Administrators*, select *Detail*. The list of current administrator sessions appears.

The following information is available:

User Name	The name of the administrator account. Your session is indicated by *(current)*.
IP Address	The IP address where the administrator is logging in from. This field also displays the logon type (GUI, jsconsole, SSH, or telnet).
Start Time	The date and time the administrator logged in.
Time Out (mins)	The maximum duration of the session in minutes (1 to 480 minutes).

The following option is available:

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* > *Dashboard*.
2. In the *System Information* widget, under *Current Administrators*, select *[Detail]*. The list of current administrator sessions opens.
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 logon screen when disconnected. They will not have any additional warning. It is a good idea to inform the administrator before disconnecting if possible should they be in the middle of important configurations for the FortiManager or another device.

Administrator

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

The following information is available:

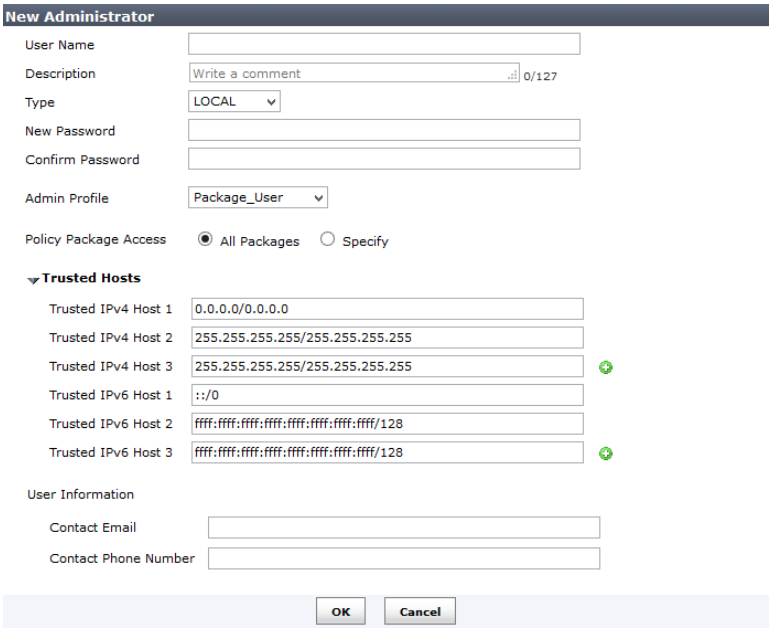
User Name	The name this administrator uses to log in. Select the administrator name to edit the administrator settings.
Type	The profile type. One of the following: LOCAL, RADIUS, LDAP, TACACS+, or PKI. When the administrator profile is a restricted administrator, this information will appear in the type column.
Profile	The administrator profile for this user that determines the permissions of this administrator. For information on administrator profiles, see Profile on page 86.
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. An enabled icon indicates the administrator is logged in, a disabled icon indicates the administrator is not logged in.
Comments	Descriptive text about the administrator account.
Email	The contact email address associated with the administrator.
Phone	The contact phone number associated with the administrator.
Trusted IPv4 Host	The IPv4 trusted host(s) associated with the administrator.
Trusted IPv6 Hosts	The IPv6 trusted host(s) associated with the administrator.

The following options are available:

Create New	Select to create a new administrator.
Edit	Select the checkbox next to the administrator, right-click, and select *Edit* in the right-click menu to edit the entry. Alternatively, you can double-click the entry to open the *Edit Administrator* page.
Delete	Select the check box next to the administrator you want to remove from the list and select *Delete*.
Column Settings	Right-click the column heading to open *Column Settings* for the administrator page. You can select to enable columns, reset columns to their default state and organize the order in which the columns are displayed.

To create a new local administrator account:

1. Go to *System Settings* > *Admin* > *Administrator* and select *Create New* in the toolbar. The *New Administrator* dialog box opens.



2. Configure the following settings:

User Name	Type the name that this administrator uses to log in. This field is available if you are creating a new administrator account.
Description	Optionally, type a description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account. Character limit: 127
Type	Select LOCAL from the drop-down list.

New Password	Type the password.
Confirm Password	Type the password again to confirm it. The passwords must match.
Admin Profile	Select a profile from the drop-down menu. The profile selected determines the administrator's permission to the FortiManager unit's features. *Restricted_User* and *Standard_User* administrator profiles do not have access to the *System Settings* tab. An administrator with either of these administrator profiles will see a change password icon in the navigation pane. To create a new profile, see Configuring administrator profiles on page 89.
Administrative Domain	Choose the ADOMs this administrator will be able to access, or select *All ADOMs*. Select *Specify* and then select the add icon to add Administrative Domains. Select the remove icon to remove an administrative domain from this list.This field is available only if ADOMs are enabled. When the *Admin Profile* is a restricted administrator profile, you can only select one administrative domain. Best practice: Restrict administrator access only to the specific ADOMs that they are responsible for.
Policy Package Access	Choose the policy packages this administrator will have access to, or select *All Package*. Select *Specify* and then select the *Add* icon to add policy packages. Select the remove icon to remove a policy package from this list.This field is not available when the *Admin Profile* is a restricted administrator profile.Best practice: Restrict administrator access only to the specific policy packages that they are responsible for.
Trusted Host	Optionally, type the trusted host IPv4 or IPv6 address and netmask from which the administrator can log in to the FortiManager unit. Select the *Add* icon to add trusted hosts. You can specify up to ten trusted hosts. Select the delete icon to remove a policy package from this list. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see Using trusted hosts on page 86. Best practice: Restrict administrator access by trusted hosts to help prevent unwanted access.
User Information (optional)	
Contact Email	Type a contact email address for the new administrator. This email address is also used for workflow session approval email notifications.
Contact Phone	Type a contact phone number for the new administrator.

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

For information on configuring restricted administrator profiles and accounts, see Restricted Administrator Profiles on page 124.

RADIUS authentication for administrators

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

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

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

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

For information on configuring a RADIUS server for remote administrator authentication, see Remote authentication server on page 90.

To create a new RADIUS administrator account:

1. Go to *System Settings* > *Admin* > *Administrator* and select *Create New* in the toolbar. The *New Administrator* dialog box opens.
2. Configure the following settings:

User Name	Type the name that this administrator uses to log in.
Description	Optionally, type a description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account. Character limit: 127
Type	Select RADIUS from the drop-down menu.
RADIUS Server	Select the RADIUS server from the drop-down menu.
Wildcard	Select to enable wildcard.
New Password	Type the password. This field is hidden when *Wildcard* is enabled.
Confirm Password	Type the password again to confirm it. The passwords must match. This field is hidden when *Wildcard* is enabled.
Admin Profile	Select a profile from the drop-down menu. The profile selected determines the administrator's permission to the FortiManager unit's features. To create a new profile, see Configuring administrator profiles on page 89.

Administrative Domain	Choose the ADOMs this administrator will be able to access, or select *All ADOMs*. Select *Specify* and then select the add icon to add Administrative Domains. Select the remove icon to remove an administrative domain from this list.This field is available only if ADOMs are enabled. When the *Admin Profile* is a restricted administrator profile, you can only select one administrative domain. Best practice: Restrict administrator access only to the specific ADOMs that they are responsible for.
Policy Package Access	Choose the policy packages this administrator will have access to, or select *All Package*. Select *Specify* and then select the *Add* icon to add policy packages. Select the remove icon to remove a policy package from this list. This field is not available when the *Admin Profile* is a restricted administrator profile. Best practice: Restrict administrator access only to the specific policy packages that they are responsible for.
Trusted Host	Optionally, type the trusted host IPv4 or IPv6 address and netmask from which the administrator can log in to the FortiManager unit. Select the *Add* icon to add trusted hosts. You can specify up to ten trusted hosts. Select the delete icon to remove a policy package from this list. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see Using trusted hosts on page 86. Best practice: Restrict administrator access by trusted hosts to help prevent unwanted access.
User Information (optional)	
Contact Email	Type a contact email address for the new administrator. This email address is also used for workflow session approval email notifications.
Contact Phone	Type a contact phone number for the new administrator.

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

Configuring LDAP authentication for administrators

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, printers, etc.

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

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

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

For information on configuring an LDAP server for remote administrator authentication, see Remote authentication server on page 90.

To create a new LDAP administrator account:

1. Go to *System Settings* > *Admin* > *Administrator* and select *Create New* in the toolbar. The *New Administrator* dialog box opens.
2. Configure the following settings:

User Name	Type the name that this administrator uses to log in.
Description	Optionally, type a description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account. Character limit: 127
Type	Select LDAP from the drop-down menu.
LDAP Server	Select the LDAP server from the drop-down menu.
Wildcard	Select to enable wildcard.
New Password	Type the password. This field is hidden when *Wildcard* is enabled.
Confirm Password	Type the password again to confirm it. The passwords must match.This field is hidden when *Wildcard* is enabled.
Admin Profile	Select a profile from the drop-down menu. The profile selected determines the administrator's permission to the FortiManager unit's features. To create a new profile, see Configuring administrator profiles on page 89.
Administrative Domain	Choose the ADOMs this administrator will be able to access, or select *All ADOMs*. Select *Specify* and then select the add icon to add Administrative Domains. Select the remove icon to remove an administrative domain from this list. This field is available only if ADOMs are enabled. When the *Admin Profile* is a restricted administrator profile, you can only select one administrative domain. Best practice: Restrict administrator access only to the specific ADOMs that they are responsible for.
Policy Package Access	Choose the policy packages this administrator will have access to, or select *All Package*. Select *Specify* and then select the *Add* icon to add policy packages. Select the remove icon to remove a policy package from this list.This field is not available when the *Admin Profile* is a restricted administrator profile. Best practice: Restrict administrator access only to the specific policy packages that they are responsible for.

Trusted Host	Optionally, type the trusted host IPv4 or IPv6 address and netmask from which the administrator can log in to the FortiManager unit. Select the *Add* icon to add trusted hosts. You can specify up to ten trusted hosts. Select the delete icon to remove a policy package from this list.Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see Using trusted hosts on page 86. Best practice: Restrict administrator access by trusted hosts to help prevent unwanted access.
User Information (optional)	
Contact Email	Type a contact email address for the new administrator. This email address is also used for workflow session approval email notifications.
Contact Phone	Type a contact phone number for the new administrator.

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

TACACS+ authentication for administrators

Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other network computing devices via one or more centralized servers.

If you have configured TACACS+ support and an administrator is required to authenticate using a TACACS+ server, the FortiManager unit contacts the TACACS+ server for authentication. If the TACACS+ server cannot authenticate the administrator, the connection is refused by the FortiManager unit.

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

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

For information on configuring a TACACS+ server for remote administrator authentication, see Remote authentication server on page 90.

To create a new TACACS+ administrator account:

1. Go to *System Settings* > *Admin* > *Administrator* and select *Create New* in the toolbar. The *New Administrator* dialog box opens.
2. Configure the following settings:

User Name	Type the name that this administrator uses to log in.
Description	Optionally, type a description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account. Character limit: 127
Type	Select TACACS+ from the drop-down menu.

TACACS+ Server	Select the TACACS+ server from the drop-down menu.
Wildcard	Select to enable wildcard.
New Password	Type the password. This field is hidden when *Wildcard* is enabled.
Confirm Password	Type the password again to confirm it. The passwords must match.This field is hidden when *Wildcard* is enabled.
Admin Profile	Select a profile from the drop-down menu. The profile selected determines the administrator's permission to the FortiManager unit's features. To create a new profile, see Configuring administrator profiles on page 89.
Administrative Domain	Choose the ADOMs this administrator will be able to access, or select *All ADOMs*. Select *Specify* and then select the add icon to add Administrative Domains. Select the remove icon to remove an administrative domain from this list. This field is available only if ADOMs are enabled. When the *Admin Profile* is a restricted administrator profile, you can only select one administrative domain. Best practice: Restrict administrator access only to the specific ADOMs that they are responsible for.
Policy Package Access	Choose the policy packages this administrator will have access to, or select *All Package*. Select *Specify* and then select the *Add* icon to add policy packages. Select the remove icon to remove a policy package from this list. This field is not available when the *Admin Profile* is a restricted administrator profile. Best practice: Restrict administrator access only to the specific policy packages that they are responsible for.
Trusted Host	Optionally, type the trusted host IPv4 or IPv6 address and netmask from which the administrator can log in to the FortiManager unit. Select the *Add* icon to add trusted hosts. You can specify up to ten trusted hosts. Select the delete icon to remove a policy package from this list. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see Using trusted hosts on page 86. Best practice: Restrict administrator access by trusted hosts to help prevent unwanted access.
User Information (optional)	
Contact Email	Type a contact email address for the new administrator. This email address is also used for workflow session approval email notifications.
Contact Phone	Type a contact phone number for the new administrator.

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

PKI certificate authentication for administrators

Public Key Infrastructure (PKI) authentication uses X.509 certificate authentication library that takes a list of peers, peer groups, and user groups and returns authentication successful or denied notifications. Administrators only need a valid X.509 certificate for successful authentication; no username or password is necessary.

To use PKI authentication for an administrator, you must configure the authentication before you create the administrator accounts. To do this you need to:

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

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

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

For information on configuring a PKI server for remote administrator authentication, see Remote authentication server on page 90.

To get the CA certificate:

1. Log into your FortiAuthenticator.
2. Go to *Certificate Management* > *Certificate Authorities* > *Local CAs*.
3. Select the certificate and select *Export* in the toolbar to save the `ca_fortinet.com` CA certificate to your management computer. The saved CA certificate's filename is `ca_fortinet.com.crt`.

To get the administrator certificate:

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

To import the administrator certificate into your browser:

1. In Mozilla Firefox, go to *Edit* > *Preferences* > *Advanced* > *Encryptions* > *View Certificates* > *Import*.
2. Select the file `admin_fortinet.com.p12` and enter the password used in the previous step.

To import the CA certificate into the FortiManager:

1. Log into your FortiManager.
2. Go to *System Settings* > *Certificates* > *CA Certificates*.
3. Select Import in the toolbar and browse for the `ca_fortinet.com.crt` file that you saved to your management computer. The certificate is displayed as *CA_Cert_1*.

To create a new PKI administrator account:

1. Go to *System Settings* > *Admin* > *Administrator* and select *Create New* in the toolbar. The *New Administrator* dialog box opens.
2. Configure the following settings:

User Name	Type the name that this administrator uses to log in. This field is available if you are creating a new administrator account.
Description	Optionally, type a description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account. (Character limit = 127)
Type	Select PKI from the drop-down list.
Subject	Type a comment in the subject field for the PKI administrator.
CA	Select the CA certificate (CA_Cert_1) from the drop-down menu.
Require two-factor authentication	Select to enable two-factor authentication.
New Password	Type the password.
Admin Profile	Select a profile from the drop-down menu. The profile selected determines the administrator's permission to the FortiManager unit's features. To create a new profile, see Configuring administrator profiles on page 89.
Administrative Domain	Choose the ADOMs this administrator will be able to access, or select *All ADOMs*. Select *Specify* and then select the add icon to add Administrative Domains. Select the remove icon to remove an administrative domain from this list. This field is available only if ADOMs are enabled. When the *Admin Profile* is a restricted administrator profile, you can only select one administrative domain. Best practice: Restrict administrator access only to the specific ADOMs that they are responsible for.
Policy Package Access	Choose the policy packages this administrator will have access to, or select *All Package*. Select *Specify* and then select the *Add* icon to add policy packages. Select the remove icon to remove a policy package from this list. This field is not available when the *Admin Profile* is a restricted administrator profile. Best practice: Restrict administrator access only to the specific policy packages that they are responsible for.

Trusted Host	Optionally, type the trusted host IPv4 or IPv6 address and netmask from which the administrator can log in to the FortiManager unit. Select the *Add* icon to add trusted hosts. You can specify up to ten trusted hosts. Select the delete icon to remove a policy package from this list. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see Using trusted hosts on page 86. Best practice: Restrict administrator access by trusted hosts to help prevent unwanted access.
User Information (optional)	
Contact Email	Type a contact email address for the new administrator.
Contact Phone	Type a contact phone number for the new administrator.

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

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

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

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

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

To modify an existing administrator account:

1. Go to *System Settings* > *Admin*> *Administrator*.
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 local administrator account: on page 76.
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 opens.
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 permissions. In addition to knowing the password, an administrator must connect only through the subnet or subnets you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

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

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

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

Profile

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

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

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

The below table lists permissions for the four predefined administrator profiles. When *Read/Write* is selected, the user can view and make changes to the FortiManager system. When *Read-Only* is selected, the user can only

view information. When *None* is selected, the user can neither view or make changes to the FortiManager system. The administrator profile restricts access to both the FortiManager GUI and command line interfaces

Setting	Predefined Administrator Profiles			
	Super User	Standard User	Restricted User	Package User
System Settings `system-setting`	Read/Write	None	None	Read-Only
Administrative Domain `adom-switch`	Read/Write	Read/Write	None	Read-Only
FortiGuard Center `fgd_center`	Read/Write	None	None	Read-Only
Device Manager `device-manager`	Read/Write	Read/Write	Read-Only	Read/Write
Add/Delete Devices/Groups `device-op`	Read/Write	Read/Write	None	Read/Write
Install To Devices `deploy-management`	Read/Write	Read/Write	Read-Only	Read/Write
Retrieve Configuration from Devices `config-retrieve`	Read/Write	Read/Write	Read-Only	Read-Only
Terminal Access `term-access`	Read/Write	Read/Write	Read-Only	Read-Only
Manage Device Configuration `device-config`	Read/Write	Read/Write	Read-Only	Read/Write
System Templates `device-profile`	Read/Write	Read/Write	Read-Only	Read/Write
Policy & Objects `policy-objects`	Read/Write	Read/Write	Read-Only	Read/Write
Global Policy Packages & Objects `global-policy-packages`	Read/Write	Read/Write	None	Read/Write
Assignment `assignment`	Read/Write	None	None	Read-Only
Policy Packages & Objects `adom-policy-packages`	Read/Write	Read/Write	Read-Only	Read/Write

Setting	Predefined Administrator Profiles			
	Super User	Standard User	Restricted User	Package User
Policy Check `consistency-check`	Read/Write	Read/Write	Read-Only	Read-Only
VPN Manager `vpn-manager`	Read/Write	Read/Write	Read-Only	Read/Write
Workflow Approve `workflow-approve`	Read/Write The administrator can approve or reject workflow sessions.	None The administrator can only view diff.	None The administrator can only view diff.	Read-Only The administrator can only view diff.
FortiView `realtime-monitor`	Read/Write	Read/Write	Read-Only	Read-Only
Event Management `event-management`	Read/Write	Read/Write	Read-Only	Read-Only
Reports `report-viewer`	Read/Write	Read/Write	Read-Only	Read-Only

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

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

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

The following information is displayed:

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 89.
Type	The profile type. Either *System Admin* or *Restricted Admin*.
Description	Provides a brief description of the system and device access permissions allowed for the selected profile.

The following options are available:

Create New	Select to create a custom administrator profile.

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

Configuring administrator profiles

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

For information on configuring restricted administrator profiles and accounts, see Restricted Administrator Profiles on page 124.

To create a custom system administrator profile:

1. Go to *System Settings* > *Admin* > *Profile* and select *Create New* in the toolbar. The *Create Profile* dialog box appears.
2. Configure the following settings:

Profile Name	Type a name for this profile.
Description	Type a description for this profile. While not a requirement, a description can help to know what the profiles is for or the levels it is set to.
Type	Select *System Admin*.
System Settings	Select *None*, *Read Only*, or *Read/Write* access.
Administrator Domain	Select *None*, *Read Only*, or *Read/Write* access.
FortiGuard Center	Select *None*, *Read Only*, or *Read/Write* access.
Device Manager	Select *None*, *Read Only*, or *Read/Write* access. Customize the individual device manager selections as needed.
Policy & Objects	Select *None*, *Read Only*, or *Read/Write* access. Customize the individual policy and objects selections as needed.

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.

Workflow Approval

The *System Settings* > *Admin* > *Workflow Approval* menu enables you to create or edit approval matrices for workflow mode. You can configure one approval matrix per ADOM. The approval matrix defines the relationship of approvers and requestors and allows you to configure who receives notifications.

This menu is only available when `workflow-mode` is set to `workflow`.

Create a new approval matrix:

1. Go to *System Settings* > *Admin* > *Workflow Approval*.
2. Select *Create New* in the toolbar. The *New Approval Matrix* page is displayed.
3. Configure the following settings:

ADOM	Select the ADOM from the drop-down list.
Approval Group	Select to add approvers to the approval group. Select the add icon to create a new approval group. Select the delete icon to remove an approval group.
Send an Email Notifcation to	Select to add admistrators to send email notifications to. Select the remove icon to remove an administrator from the field.
Mail Server	Select the mail server from the drop-down list.

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

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 LDAP remote authentication servers can be added and linked to all ADOMs or specific ADOMs. Existing servers can be modified and deleted as required; see Manage remote authentication servers on page 93.

The following information is displayed:

Name	The name of the server.
Type	The server type. One of LDAP, RADIUS, or TACACS+.

ADOM	The administrative domain(s) which are linked to the remote authentication server.
Details	Details about the server, such as the IP address.

The following options are available:

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

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.

For information on configuring a TACACS+ server for remote administrator authentication, see Configuring LDAP authentication for administrators on page 79.

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.
3. Configure the following information:

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

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

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 type a user name and password. This information is passed to a RADIUS server, which authenticates the user and authorizes access to the network.

You can create or edit RADIUS server entries in the server list to support authentication of administrators. When an administrator account's type is set to RADIUS, the FortiManager unit uses the RADIUS server to verify the administrator password at logon. The password is not stored on the FortiManager unit.

For information on configuring a TACACS+ server for remote administrator authentication, see RADIUS authentication for administrators on page 78.

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.
3. Configure the following settings:

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

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

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

TACACS+

TACACS+ allows a client to accept a user name and password and send a query to a TACACS+ authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies network access to the user. The default TCP port for a TACACS+ server is 49.

For information on configuring a TACACS+ server for remote administrator authentication, see TACACS+ authentication for administrators on page 81.

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.
3. Configure the following information:

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

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

  In order to improve security, you can change the default port configurations for administrative connections to the FortiManager. When connecting to the FortiManager unit when the port has changed, the port must be included, such as `https://<ip_address>:<port>`. For example, if you are connecting to the FortiManager unit using port 8080, the URL would be `https://192.168.1.99:8080`. When you change to the default port number for HTTP, HTTPS, Telnet, or SSH, ensure that the port number is unique.
- Idle Timeout settings

  By default, the GUI disconnects administrative sessions if no activity occurs for five minutes. This prevents someone from using the GUI if the management computer is left unattended.
- Language of the GUI

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

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

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

To configure the administrative settings:

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

Administration Settings	
HTTP Port	Type the TCP port to be used for administrative HTTP access. Select to redirect to HTTPS. Default port: 80
HTTPS Port	Type the TCP port to be used for administrative HTTPS access. Default port: 443
HTTPS & Web Service Server Certificate	Select a certificate from the drop-down list.
Idle Timeout	Type the number of minutes that an administrative connection can be idle before the administrator must log in again. The maximum is 480 minutes (8 hours). To ensure security, the idle timeout should be a short period of time to avoid the administrator inadvertently leaving the management computer logged in to the FortiManager unit and opening the possibility of someone walking up and modifying the network options. Range: 1 to 480 (minutes)
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. Range: 8 to 32 (characters)
Must Contain	Select the types of characters that a password must contain. Select from the following options: • Upper Case Letters • Lower Case Letters • Numbers (0-9) • Special Characters or Non-alphanumeric Letters
Admin Password Expires after	Select the number of days that a password is valid for, after which time it must be changed.
Display Options on GUI	Select the required options from the list.
Show VPN Console	Select to display the VPN Console menu item. This menu is located in the *Policy & Objects* tab under Policy Package in the left-hand tree menu. VPN Console is available when ADOM *VPN Management* is set to *Central VPN Console*. This is an advanced FortiManager feature.
Show Script	Select to display the *Script* menu item. This menu is located in the *Device Manager* tab under *Devices & Groups* in the left-hand tree menu. This is an advanced FortiManager feature.

Show Device List Import/Export	Select to display the *Import Device List* and *Export Device List* buttons. These buttons are located in the *Device Manager* tab in the toolbar. This is an advanced FortiManager feature.
Show Add Multiple Button	Select to display the *Add Multiple* button. This button is located in the *Device Manager* tab in the toolbar. This is an advanced FortiManager feature.

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

Administrator password retries and lockout duration

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

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

To configure the lockout options:

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

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

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

Configure two-factor authentication for administrator log on

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

- FortiManager
- FortiAuthenticator
- FortiToken

FortiAuthenticator side configuration

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

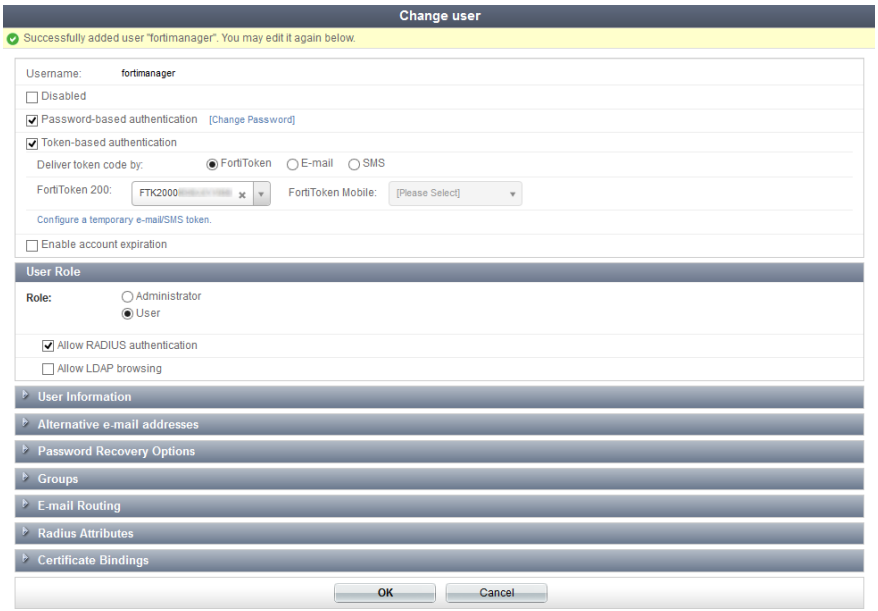
Create a local user:

1. Go to *Authentication* > *User Management* > *Local Users*.
2. Select *Create New* in the toolbar. The *Create New User* page opens.

3. Configure the following settings:

Username	Type a user name for the local user.
Password creation	Select Specify a password from the drop-down list.
Password	Type a password. The password must be a minimum of 8 characters.
Password confirmation	Type the password again. The passwords must match.
Enable account expiration	Optionally, select to enable account expiration. For more information see the *FortiAuthenticator Administration Guide*.

4. Select *OK* to continue. The *Change user* page opens.



5. Configure the following settings:

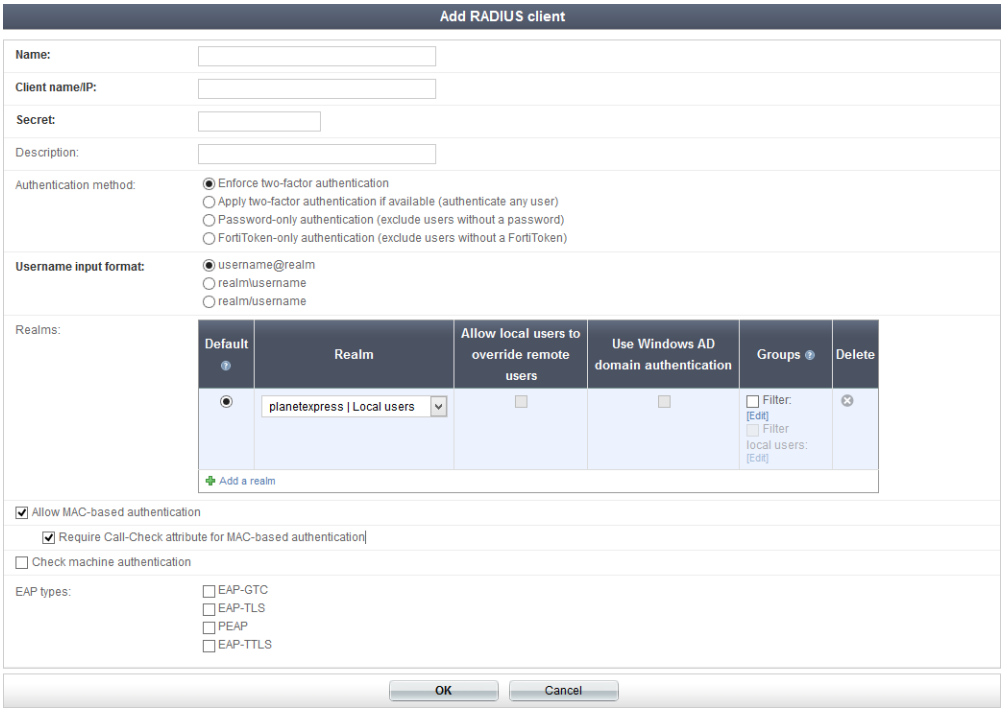
Disabled	Select to disable the local user.
Password-based authentication	Leave this option selected. Select *[Change Password]* to change the password for this local user.
Token-based authentication	Select to enable token-based authentication.
Deliver token code by	Select to deliver token by FortiToken.
FortiToken 200	Select the FortiToken from the drop-down list.
Enable account expiration	Optionally, select to enable account expiration. For more information see the *FortiAuthenticator Administration Guide*.
User Role	
Role	Select either Administrator or User.

Allow RADIUS authentication	Select to allow RADIUS authentication.
Allow LDAP browsing	Optionally, select to allow LDAP browsing. For more information see the *FortiAuthenticator Administration Guide*.

6. Select *OK* to save the setting.

Create a RADIUS client:

1. Go to *Authentication* > *RADIUS Service* > *Clients*.
2. Select *Create New* in the toolbar. The *Create New RADIUS Client* page opens.



3. Configure the following settings:

Name	Type a name for the RADIUS client entry.
Client name/IP	Type the IP address or FQDN of the FortiManager.
Secret	Type the server secret. This value must match the FortiManager RADIUS server setting at *System Settings* > *Admin* > *Remote Auth Server*.
Description	Type an optional description for the RADIUS client entry.
Authentication method	Select *Enforce two-factor authentication* from the list of options.
Username input format	Select specific user name input formats.

Realms	Realm configuration. For more information see the *FortiAuthenticator Administration Guide*.
Allow MAC-based authentication	Optional configuration. For more information see the *FortiAuthenticator Administration Guide*.
EAP types	Optional configuration. For more information see the *FortiAuthenticator Administration Guide*.

4. Select *OK* to save the setting.

FortiManager side configuration

Configure the RADIUS server:

1. Go to *System Settings* > *Admin* > *Remote Auth Server*.
2. Select *Create New* in the toolbar and select *RADIUS* from the drop-down list. The *New RADIUS Server* page opens.
3. Configure the following settings:

Name	Type a name to identify the FortiAuthenticator.
Server Name/IP	Type the IP address or fully qualified domain name of your FortiAuthenticator.
Server Secret	Type the FortiAuthenticator secret.
Secondary Server Name/IP	Type the IP address or fully qualified domain name of the secondary FortiAuthenticator, if applicable.
Secondary Server Secret	Type the secondary FortiAuthenticator secret, if applicable.
Port	Type the port for FortiAuthenticator traffic. The default port is 1812.
Auth-Type	Select the authentication type the FortiAuthenticator requires. The default setting of *ANY* has the FortiManager unit try all the authentication types. Select one of: *ANY*, *PAP*, *CHAP*, or *MSv2*.

4. Select *OK* to save the setting.

Create the administrator users:

See RADIUS authentication for administrators on page 78 for instruction on creating a new RADIUS administrator.

Test the configuration:

1. Attempt to log into the FortiManager GUI with your new credentials.
2. Type your user name and password and select Login.
3. The FortiToken page is displayed.
4. Type your FortiToken pin code and select *Submit* to finish logging in to FortiManager.

Certificates

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

Local certificates are issued for a specific server, or website. Generally they are very specific, and often for an internal enterprise network.

CA root certificates are similar to local certificates, however they apply to a broader range of addresses or to an entire company.

The CRL is a list of certificates that have been revoked and are no longer usable. This list includes certificates that have expired, been stolen, or otherwise compromised. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and includes the date and time when the next CRL will be issued as well as a sequence number to help ensure you have the most current version of the CRL.

Go to *System Settings* > *Certificates* to view FortiManager local certificates, CA certificates and CRLs.

The following information is displayed:

Certificate Name	Displays the certificate name.
Subject	Displays the certificate subject information.
Status	Displays the certificate status. Select *View Certificate Detail* to view additional certificate status information.

The following options are available:

Create New	Select to create a new certificate request.
View	Select the checkbox next to the certificate, right-click, and select *View* in the right-click menu to view the entry.
Delete	Select the checkbox next to a certificate entry and select *Delete* to remove the certificate selected. Select *OK* in the confirmation dialog box to proceed with the delete action. Delete is also available in the right-click menu.
Import	Select to import a local certificate. Browse for the local certificate on the management computer and select *OK* to complete the import.
View Certificate Detail	Select the checkbox next to a certificate entry and select *View Certificate Detail* to view certificate details.
Download	Select the checkbox next to a certificate entry and select *Download* to download the certificate to your local computer.

Creating a local certificate

To create a certificate request:

1. Go to *System Settings* > *Certificates* > *Local Certificates*.
2. Select *Create New* in the toolbar. The *New Certificate* window opens.
3. Enter the following information as required.

Certificate Name	The name of the certificate.
Key Size	Select the key size from the drop-down list. Select one of the following: 512 Bit, 1024 Bit, 1536 Bit, or 2048 Bit.
Common Name (CN)	Type the common name of the certificate.
Country (C)	Select the country from the drop-down list.
State/Province (ST)	Type the state or province.
Locality (L)	Type the locality.
Organization (O)	Type the organization for the certificate.
Organization Unit (OU)	Type the organization unit.
E-mail Address (EA)	Type the email address.

4. Select *OK* to save the certificate request.

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

Only local certificates can be created. CA Certificates and CRLs can only be imported

Importing certificates

To import a local certificate:

1. Go to *System Settings* > *Certificates* > *Local Certificates*.
2. Select the *Import* button in the toolbar.
3. Type the location of the local certificate, or select *browse* and browse to the location of the certificate, then select *OK*.

To import a CA certificate:

1. Go to *System Settings* > *Certificates* > *CA Certificates*.
2. Select the *Import* button in the toolbar.
3. Type the location of the local certificate, or select *browse* and browse to the location of the certificate, then select *OK*.

Importing CRLs

A CRL is a list of the CA certificate subscribers paired with certificate status information. The list contains the revoked certificates and the reason or reasons for their revocation. It also records the certificate issue dates and the CAs that issued them.

When configured to support SSL VPNs, the FortiManager unit uses the CRL to ensure that the certificates belonging to the CA and remote peers or clients are valid. You must download the CRL from the CA website on a regular basis.

To import a CRL:

1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the *Import* button in the toolbar.
3. Type the location of the certificate, or select *browse* and browse to the location of the certificate, then select *OK*.

Viewing certificate details

To view a local certificate:

1. Go to *System Settings* > *Certificates* > *Local Certificates*.
2. Select the certificates which you would like to see details about and click on *View Certificate Detail* in the toolbar. The following information is displayed:

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.

3. Select *OK* to continue.

To view a CA certificate:

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

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

To view a CRL:

1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the certificates which you would like to see details about and click on *View Certificate Detail* in the toolbar. 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* > *Certificates* > *Local Certificates*.
2. Select the certificates which you would like to download, click on *Download* in the toolbar, and save the certificate to the desired location.

To download a CA certificate:

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

Event log

The logs created by FortiManager are viewable within the GUI. You can use the *FortiManager Log Message Reference*, available from the Fortinet Document Library to interpret the messages. You can view log messages in the FortiManager GUI that are stored in memory or on the internal hard disk.

To view the log messages:

1. Go to *System Settings* > *Event Log*. The event log window opens.
2. The following information and options are available:

Clear Filter	Select to clear all column filters. This option is only displayed when a column filter has been enabled.
Historical Log	Select *Historical Log* to view historical event logs. You can view select Event Log, FDS Upload Log, or FDS Download Log from the drop-down menu. You can select to clear or view logs. The following columns are displayed: *File Name*, *Size*, and *Last Access Time*.
Download	Select *Download* to download a file containing the logs in either CSV or the normal format. Select *OK* to save the file to your management computer.

Raw Log	Select the *Raw Log/Formatted Table* button to change the log message view. Raw logs are displayed in the following format: `2013-10-17 14:26:01 log_id=0001013001 type=event subtype=fgfm pri=warning adom=n/a user=fgfm msg="fgfm connection to device FG300B3907600039 is down"`
Refresh	Select *Refresh* to refresh the displayed logs.
Column Settings	Right-click the column heading to open *Column Settings* for the event log page. You can select to enable columns, reset columns to their default state and organize the order in which the columns are displayed.
#	The event log entry identifier.
Date	The date that the log was generated. You can select the filter icon to select a specific date range to view specific log entries. Select *[Clear All Filters]* to clear all filters that have been configured. When a filter is enabled, the filter icon is green. To remove or disable a filter, select the filter icon to open the *Filter Settings* dialog box and uncheck the *Enabled* checkbox. Format: YYYY-MM-DD
Time	The time that the log was generated. You can select the filter icon to select a specific date range to view specific log entries. Select *[Clear All Filters]* to clear all filters that have been configured. When a filter is enabled, the filter icon is green. To remove or disable a filter, select the filter icon to open the *Filter Settings* dialog box and uncheck the *Enabled* checkbox. Format: HH:MM:SS
Level	The logging level of the log generated. You can select the filter icon to select a specific date range to view specific log entries. Select *[Clear All Filters]* to clear all filters that have been configured. When a filter is enabled, the filter icon is green. To remove or disable a filter, select the filter icon to open the *Filter Settings* dialog box and uncheck the *Enabled* checkbox. The logging levels are *Emergency*, *Alert*, *Critical*, *Error*, *Warning*, *Notice*, *Information*, and *Debug*.
User	The user associated with the log generated. You can select the filter icon to select a specific date range to view specific log entries. Select *[Clear All Filters]* to clear all filters that have been configured. When a filter is enabled, the filter icon is green. To remove or disable a filter, select the filter icon to open the *Filter Settings* dialog box and uncheck the *Enabled* checkbox.

Sub Type	The logging subtype of the log generated. You can select the filter icon to select a specific date range to view specific log entries. Select *[Clear All Filters]* to clear all filters that have been configured. When a filter is enabled, the filter icon is green.. To remove or disable a filter, select the filter icon to open the *Filter Settings* dialog box and uncheck the *Enabled* checkbox. The logging subtypes are System manager event, FG-FM protocol event, Device configuration event, Global database event, Script manager event, Web portal event, Firewall objects event, Policy console event, VPN console event, Endpoint manager event, Revision history event, Deployment manager event, HA event, Firmware manager event, FortiGuard service event, FortiClient manager event, FortiMail manager event, Debug I/O log event, Configuration change event, Device manager event, and Web service event.
Message	The log event message. You can select the filter icon to select a specific date range to view specific log entries. Select *[Clear All Filters]* to clear all filters that have been configured. When a filter is enabled, the filter icon is green. To remove or disable a filter, select the filter icon to open the *Filter Settings* dialog box and uncheck the *Enabled* checkbox.
Pagination	Browse pages in the event log page. You can select the number of log entries to display from the drop-down menu.

3. Select the filter icon in the heading of any of the table columns to open the *Filter Settings* window.
4. Adjust the filter settings as needed, then select *Apply* to apply the filter to the table.
5. Select *Clear Filter* from the event log table view to remove any applied filters.

Task monitor

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

Go to *System Settings* > *Task Monitor*, then select a task category from the *View* field drop-down list, or leave as the default *All*. Select a column header to sort the table by that column.

The following information is displayed:

ID	The identification number for a task.
Source	The platform from where the task is performed. The source includes the following: Package Clone, Import Wizard, System checkpoint, Install Configuration, Device Manager.
Description	The nature of the task.
User	The users who have performed the tasks.

Status	The status of the task (hover over the icon to view the description): • *All*: All types of tasks. • *Done*: Completed with success. • *Error*: Completed without success. • *Cancelled*: User cancelled the task. • *Cancelling*: User is cancelling the task. • *Aborted*: The FortiManager system stopped performing this task. • *Aborting*: The FortiManager system is stopping performing this task. • *Running*: Being processed. In this status, a percentage bar appears in the Status column.
Start Time	The date and time that the task was performed.
ADOM	The ADOM to which the task applies.

The following options are available:

Delete	Remove the selected task or tasks from the list.
View	Select which tasks to view from the drop-down list, based on their status. The available options are: *Running*, *Pending*, *Done*, *Error*, *Cancelling*, *Cancelled*, *Aborting*, *Aborted*, *Warning*, and *All*. Default: All
Expand Arrow	Select the expand arrow icon to display the specific actions taken under this task. To filter the specific actions taken for a task, select one of the options on top of the action list. Select the history icon to view specific information on task progress. This can be useful when troubleshooting warnings and errors.
Group Error Devices	Select *Group Error Devices* to create a group of the devices that failed, allowing for re-installations to easily be done on only the failed devices.
View Script Execution History	For script execution tasks, the log of the script can be viewed be selecting the *View Script Execution History* icon.The log shows the script itself, and the results of running the script. See Scripts on page 218.
Pagination	Browse pages in the task monitor page. You can select the number of task entries to display from the drop-down menu.

Advanced

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

SNMP	Select to configure FortiGate and FortiManager reporting through SNMP traps.
Mail server	Select to configure mail server settings for alerts, edit existing settings, or delete mail servers.
Syslog server	Select to configure syslog server settings for alerts, edit existing settings, or delete syslog servers.
Meta fields	Select to configure metadata fields for FortiGate objects, and for FortiGate-5000 series shelf managers.
Device log settings	Select to configure log settings and access. This menu is available when *FortiAnalyzer Features* is enabled.
File management	FortiManager allows you to configure automatic deletion of device log files, quarantined files, reports, and content archive files after a set period of time. This menu is available when *FortiAnalyzer Features* is enabled.
Advanced settings	Select to configure global advanced settings such as offline mode, device synchronization settings and install interface policy only.
Portal users	Select to create web portal users for FortiManager APIs.

SNMP

SNMP is a method for a FortiManager system to monitor and report on FortiGate devices. It also can allow you to monitor a FortiManager system on your local computer. You will need an SNMP agent on your computer to read the SNMP information.

Using SNMP, your FortiManager system checks the attached FortiGate devices for their system health, traffic levels, and many other details. By default when a FortiGate device is initially configured on your FortiManager system, that FortiGate device's SNMP settings are configured to report to the FortiManager system.

Go to *System Settings* > *Advanced* > *SNMP* to configure your FortiManager system's SNMP settings.

SNMP has two parts - the SNMP agent or the device that is sending traps, and the SNMP manager that monitors those traps. The SNMP communities on the monitored FortiGate devices are hard coded and configured by the FortiManager system - they are not user configurable.

The FortiManager SNMP implementation is read-only — SNMP v1, v2c, and v3 compliant SNMP manager applications, such as those on your local computer, have read-only access to FortiManager system information and can receive FortiManager system traps.

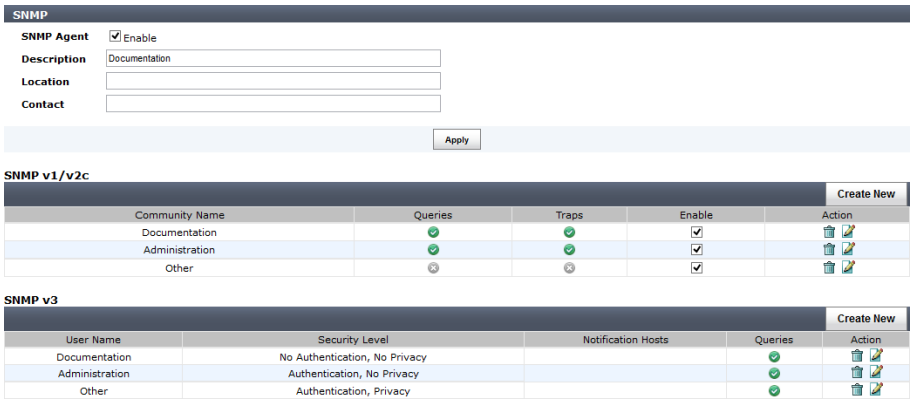
Configuring the SNMP agent

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

The SNMP manager can monitor the FortiManager system to determine if it is operating properly, or if there are any critical events occurring. The description, location, and contact information for this FortiManager system will

be part of the information an SNMP manager will have — this information is useful if the SNMP manager is monitoring many devices, and it will enable faster responses when the FortiManager system requires attention.

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



The following information and options are available:

SNMP	
SNMP Agent	Select to enable the FortiManager SNMP agent. When this is enabled, it sends FortiManager SNMP traps.
Description	Type a description of this FortiManager system to help uniquely identify this unit.
Location	Type the location of this FortiManager system to help find it in the event it requires attention.
Contact	Type the contact information for the person in charge of this FortiManager system.
SNMP v1/2c	The list of SNMP v1/v2c communities added to the FortiManager configuration.
Create New	Select *Create New* to add a new SNMP community. If SNMP agent is not selected, this control will not be visible.
Community Name	The name of the SNMP community.
Queries	The status of SNMP queries for each SNMP community. The enabled icon indicates that at least one query is enabled. The disabled icon indicates that all queries are disabled.
Traps	The status of SNMP traps for each SNMP community. The enabled icon indicates that at least one trap is enabled. The disabled icon indicates that all traps are disabled.
Enable	Select to enable or deselect to disable the SNMP community.

	Action	Select the delete icon to remove an SNMP community.Select the edit icon to edit an SNMP community.
SNMP v3		The list of SNMPv3 users added to the configuration.
	Create New	Select *Create New* to add a new SNMP community. If SNMP agent is not selected, this control will not be visible. For more information, see Configuring a SNMPv3 user on page 110.
	User Name	The user name for the SNMPv3 user.
	Security Level	The security level assigned to the SNMPv3 user.
	Notification Hosts	The notification host or hosts assigned to the SNMPv3 user.
	Queries	The status of SNMP queries for each SNMP user. The enabled icon indicates that query is enabled. The disabled icon indicates query is disabled.
	Action	Select the delete icon to remove an SNMP community. Select the edit icon to edit an SNMP community.

Configuring an SNMP v1/v2c community

An SNMP community is a grouping of equipment for network administration purposes. Add SNMP communities so that the FortiManager system (the SNMP agent in this case) can connect to the SNMP manager that is monitoring.

These SNMP communities do not refer to the FortiGate devices the FortiManager system is managing.

Each community can have a different configuration for SNMP traps and can be configured to monitor different events. You can add the IP addresses of up to eight hosts to each community. Hosts can receive SNMP device traps and information.

Select *Create New* in the SNMP v1/v2c toolbar to open the *New SNMP Community* page, where you can configure a new SNMP community.

When you create a new SNMP community, there are no host entries. Selecting *Add* creates an entry that broadcasts the SNMP traps and information to the network connected to the specified interface.

Configure the following settings:

Community Name	Type a name to identify the SNMP community. If you are editing an existing community, you will be unable to change the name.
Hosts	The list of hosts that can use the settings in this SNMP community to monitor the FortiManager system. Select *Add* to create a new entry that you can edit.

	IP Address	Type the IP address of an SNMP manager. By default, the IP address is 0.0.0.0 so that any SNMP manager can use this SNMP community.
	Interface	Select the name of the interface that connects to the network where this SNMP manager is located from the drop-down list. You need to do this if the SNMP manager is on the Internet or behind a router.
	Delete	Select the delete icon to remove this SNMP manager entry.
	Add	Select to add a new default entry to the Hosts list that you can edit as needed. You can have up to eight SNMP manager entries for a single community.
Queries		Type the port number that the FortiManager system uses to send SNMPv1 and SNMPv2c queries to the FortiManager in this community. Enable queries for each SNMP version that the FortiManager system uses. Default port: 161
Traps		Type the Remote port number that the FortiManager system uses to send SNMPv1 and SNMPv2c traps to the FortiManager in this community. Enable traps for each SNMP version that the FortiManager system uses. Default port: 162
SNMP Event		Enable the events that will cause the FortiManager unit to send SNMP traps to the community. FortiManager SNMP events: • *Interface IP changed* • *Log disk space low* • *CPU Overusage* • *Memory Low* • *System Restart* • *CPU usage exclude NICE threshold* • *HA Failover* • *RAID Event*: This SNMP event is available for devices which support RAID. • *Power Supply Failed* FortiAnalyzer feature set SNMP events: • *High licensed device quota* • *High licensed log GB/day* • *Log Alert* • *Log Rate* • *Data Rate*

Configuring a SNMPv3 user

The FortiManager SNMPv3 implementation includes support for queries, traps, authentication, and privacy. Select *Create New* in the SNMPv3 toolbar to open the *New SNMP User* page, where you can configure a new SNMP user.

Configure the following settings:

User Name	The name of the SNMPv3 user.
Security Level	The security level of the user. Select one of the following: • No Authentication, No Privacy • Authentication, No Privacy Select the authentication algorithm (SHA1, MD5) and enter the password. • Authentication, Privacy Select the authentication algorithm (SHA1, MD5), the private algorithm (AES, DES) and enter the password.
Notification Hosts	The IP address or addresses of the host. Select the add icon to add multiple IP addresses.
Queries	Select to enable queries, then enter the port number (default: 161).
SNMP Event	Enable the events that will cause the FortiManager unit to send SNMP traps to the community. FortiManager SNMP events: • *Interface IP changed* • *Log disk space low* • *CPU Overusage* • *Memory Low* • *System Restart* • *CPU usage exclude NICE threshold* • *HA Failover* • *RAID Event*: This SNMP event is available for devices which support RAID. • *Power Supply Failed* FortiAnalyzer feature set SNMP events: • *High licensed device quota* • *High licensed log GB/day* • *Log Alert* • *Log Rate* • *Data Rate*

You can edit and delete existing SNMPv3 users.

SNMP MIBs

Fortinet device SNMP agents support Fortinet proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiManager unit configuration.

RFC support for SNMP v3 includes Architecture for SNMP Frameworks (RFC 3411), and partial support of User-based Security Model (RFC 3414).

The Fortinet and FortiManager MIBs are listed in SNMP MIBs along with the two RFC MIBs. You can obtain these MIB files from Customer Service & Support. To be able to communicate with the SNMP agent, you must compile all of these MIBs into your SNMP manager. Generally your SNMP manager will be an application on your local computer.

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

You can download the FortiManager MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager 5.00 file folder.

MIB file name or RFC	Description
FORTINET-CORE-MIB.mib	The proprietary Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor Fortinet unit configuration settings and receive traps from the Fortinet SNMP agent. For more information, see Appendix A - SNMP MIB Support on page 419 and Fortinet & FortiManager MIB fields on page 113.
FORTINET-FORTIMANAGER-MIB.mib	The proprietary FortiManager MIB includes system information and trap information for FortiManager units.
RFC-1213 (MIB II)	The Fortinet SNMP agent supports MIB II groups with the following exceptions. • No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all Fortinet traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB.
RFC-2665 (Ethernet-like MIB)	The Fortinet SNMP agent supports Ethernet-like MIB information with the following exception. No support for the dot3Tests and dot3Errors groups.

SNMP traps

Fortinet devices share SNMP traps, but each type of device also has traps specific to that device. For example FortiManager units have FortiManager specific SNMP traps. To receive Fortinet device SNMP traps, you must load and compile the FORTINET-CORE-MIB into your SNMP manager.

Traps sent include the trap message as well as the unit serial number (fnSysSerial) and host name (sysName). The Trap Message column includes the message included with the trap as well as the SNMP MIB field name to help locate the information about the trap.

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

Trap message	Description

CPU usage high (fnTrapCpuThreshold)	CPU usage exceeds the set percent. This threshold can be set in the CLI using the following commands:
	`config system snmp sysinfo`
	`set trap-high-cpu-threshold <percentage value>`
	`end`

CPU usage excluding NICE processes (fmSysCpuUsageExcludedNice)	CPU usage excluding NICE processes exceeds the set percentage. This threshold can be set in the CLI using the following commands:
	`config system snmp sysinfo`
	`set trap-cpu-high-exclude-nice-threshold <percentage value>`
	`end`

Memory low (fnTrapMemThreshold)	Memory usage exceeds 90 percent. This threshold can be set in the CLI using the following commands:
	`config system snmp sysinfo`
	`set trap-low-memory-threshold <percentage value>`
	`end`

Log disk too full (fnTrapLogDiskThreshold)	Log disk usage has exceeded the configured threshold. Only available on devices with log disks.
Temperature too high (fnTrapTempHigh)	A temperature sensor on the device has exceeded its threshold. Not all devices have thermal sensors. See manual for specifications.
Voltage outside acceptable range (fnTrapVoltageOutOfRange)	Power levels have fluctuated outside of normal levels. Not all devices have voltage monitoring instrumentation.
Power supply failure (fnTrapPowerSupplyFailure)	Power supply failure detected. Not available on all models. Available on some devices which support redundant power supplies.
Interface IP change (fnTrapIpChange)	The IP address for an interface has changed. The trap message includes the name of the interface, the new IP address and the serial number of the Fortinet unit. You can use this trap to track interface IP address changes for interfaces with dynamic IP addresses set using DHCP or PPPoE.

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

SNMP manager and browsing the Fortinet MIB fields.

MIB field	Description
fnSysSerial	Fortinet unit serial number.

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.

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

MIB field	Description
fmModel	A table of all FortiManager models.
fmTrapHASwitch	The FortiManager HA cluster has been re-arranged. A new master has been selected and asserted.

Mail server

Configure SMTP mail server settings for event management, edit existing settings, or delete mail servers.

If an existing mail server is used in an event handler, the delete icon is removed and the mail server entry cannot be deleted.

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

The following information is displayed:

SMTP Server	The name that was configured for the SMTP mail server entry.

SMTP Server Port	The SMTP server port number. Default port: 25
E-Mail Account	The E-Mail account associated with the SMTP server.
Password	The password associated with the SMTP server.

The toolbar includes the following options:

Create New	Select to create a new SMTP mail server entry.
Delete	Select to delete the SMTP mail server selected.

Right-clicking on a mail server entry in the tree menu opens a menu with the following options:

Create New	Select to create a new SMTP mail server entry.
Delete	Select to delete the SMTP mail server selected.
Test	Select to test the mail server entry. A *Test SMTP Server* dialog box is displayed. Type an email address in the dialog box and select *OK*. A test email is sent to the email address entered and a confirmation message window will be displayed with the status of the test. Select *OK* to close the window.

To create a new mail server:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Select *Create New* in the toolbar. The *Mail Server Settings* window opens.
3. Configure the following settings:

SMTP Server	Type the SMTP server domain information, e.g. mail@company.com.
SMTP Server Port	Type the SMTP server port number. D efault port: 25
Enable Authentication	Select to enable authentication.
Email Account	Type an email account, e.g. administrator@company.com.
Password	Type the email account password.

4. Select *OK* to save the setting.

To edit a mail server:

1. Go to *System Settings* > *Advanced* > *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 test the mail server:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Select an entry in the list, right-click, and select *Test* from the menu. The *Test SMTP Server* dialog box opens.
3. Type the email address that you would like to send a test email to and select *OK*. A confirmation or failure message will be displayed. Select *OK* to close the confirmation dialog box.

To delete a mail server:

1. Go to *System Settings* > *Advanced* > *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 used in an event handler, the delete icon is removed and the syslog server entry cannot be deleted.

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

The following information is displayed:

Name	The name that was configured for the syslog server entry.
IP or FQDN : Port	The IP address or FQDN and port number of the syslog server.

The toolbar includes the following options:

Create New	Select to create a new syslog server entry.
Delete	Select to delete the syslog server selected.

Right-clicking on a syslog server entry in the tree menu opens a menu with the following options:

Create New	Select to create a new syslog server entry.
Delete	Select to delete the syslog server selected.
Test	Select to test the syslog server entry. A test log is sent to the syslog server selected and a confirmation message window will be displayed with the status of the test. Select *OK* to close the window.

To create a new syslog server:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Select *Create New* in the toolbar. The *New Syslog Server* window opens.
3. Configure the following settings and then select *OK*:

Name	Type a name for the syslog server.
IP address (or FQDN)	Type the IP address or FQDN of the syslog server.
Port	Type the syslog server port number. Default port: 514

To edit a syslog server:

1. Go to *System Settings* > *Advanced* > *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 test the syslog server:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Select an entry in the list, right-click, and select *Test* from the menu. A confirmation or failure message will be displayed.
3. Select *OK* to close the confirmation dialog box.

To delete a syslog server:

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

Meta fields

The *System Setting* > *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.

Go to *System Settings* > *Advanced* > *Meta Fields* to add metadata fields for system-wide or FortiGate objects. The list of metadata fields opens.

The following information is available:

Meta Fields	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.

The following options are available in the toolbar:

Delete	Select to delete this metadata field. The default meta fields cannot be deleted.
Create New	Create a new metadata field for this object.

Right-clicking on a meta field entry in the tree menu opens a menu with the following options:

Delete	Select to delete this metadata field. The default meta fields cannot be deleted.
Edit	Select to edit an existing metadata field for this object.

To add a new metadata field:

1. Go to *System Settings* > *Advanced* > *Meta Fields*. The list of configured meta data objects opens.
2. Select *Create New*. The *Add Meta-field* dialog box opens.
3. Configure the following settings:

Object	The object to which this metadata field applies. Select one of the following: System Administrators, Devices, Device Groups, Administrative Domain, Firewall Addresses, Firewall Address Groups, Firewall Services, Firewall Service Groups, and Firewall Policy.
Name	Type 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. This field is only available for non-firewall objects. The default setting is *Enabled*.

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

To edit a metadata field:

1. Go to *System Settings* > *Advanced* > *Meta Fields.*
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 S*ystem Settings* > *Advanced* > *Meta Fields*.
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.

Device log settings

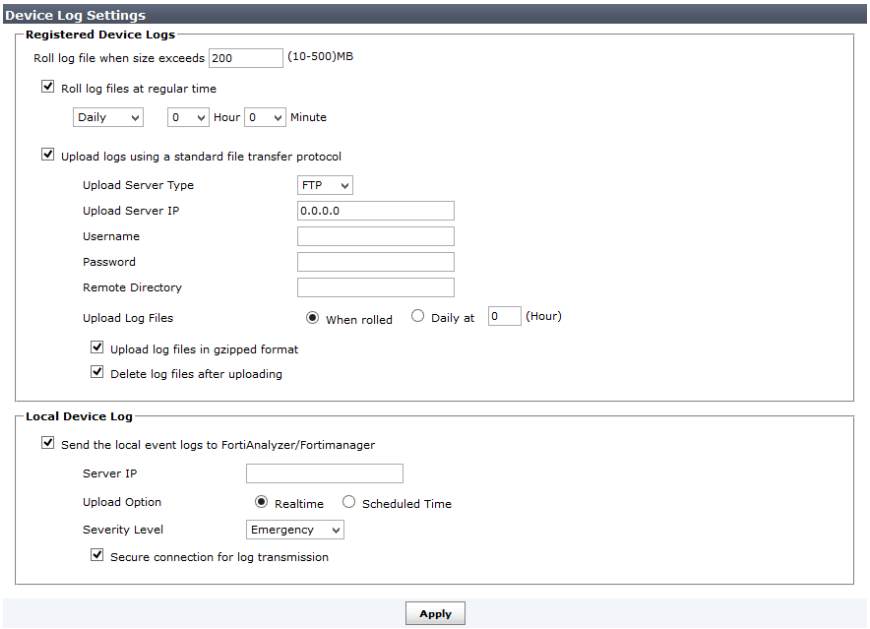
The FortiManager allows you to log system events to disk.

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

- Log rotation settings
- Log uploading

This feature is available in the GUI when *FortiAnalyzer Features* is enabled. For more information, see Enable or disable FortiAnalyzer features on page 54.

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



Configure the following settings and then select *Apply*:

Registered Device Logs	
Roll log file when size exceeds	Enter the log file size. • Range: 10 to 500 MB • Default: 200 MB
Roll log files at a regular time	Select to roll logs daily or weekly. When selecting daily, select the hour and minute value in the drop-down lists. When selecting weekly, select the day, hour, and minute value in the drop-down lists.

Upload logs using a standard file transfer protocol	Select to upload logs and configure the following settings.
Upload Server Type	Select one of *FTP, SFTP*, or *SCP*.
Upload Server IP	Enter the IP address of the upload server.
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.
Upload Log Files	Select to upload log files when they are rolled according to settings selected under *Roll Logs* or daily at a specific hour.
Upload rolled files in gzipped format	Select to gzip the logs before uploading. This will result in smaller logs, and faster upload times.
Delete files after uploading	Select to remove device log files from the FortiManager system after they have been uploaded to the Upload Server.
Local Device Log	
Send the local event logs to FortiAnalyzer / FortiManager	Select to send local event logs to another FortiAnalyzer or FortiManager device.
Server IP	Enter the IP address of the FortiAnalyzer or FortiManager.
Upload Option	Select to upload logs realtime or at a scheduled time. When selecting a scheduled time, you can specify the hour and minute to upload logs
Severity Level	Select the minimum log severity level from the drop-down list.
Secure connection for log transmission	Select to use a secure connection for log transmission.

File management

FortiManager allows you to configure automatic deletion of device log files, quarantined files, reports, and content archive files after a set period of time.

To configure automatic deletion settings, go to *System Settings* > *Advanced* > *File Management*.

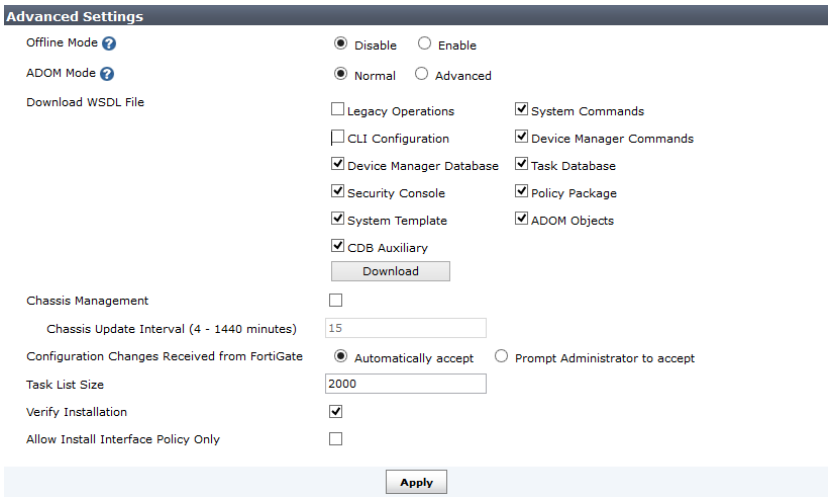
This feature is available in the GUI when *FortiAnalyzer Features* is enabled. For more information, see Enable or disable FortiAnalyzer features on page 54.

Configure the following settings:

Device log files older than	Select to enable this feature, type a value in the text field, and select the time period from the drop-down list.
Quarantined files older than	Select to enable this feature, type a value in the text field, and select the time period from the drop-down list.
Reports older than	Select to enable this feature, type a value in the text field, and select the time period from the drop-down list.
Content archive files older than	Select to enable this feature, type a value in the text field, and select the time period from the drop-down list.

Advanced settings

To view and configure advanced settings options, go to the *System Settings* > *Advanced* > *Advanced Settings* page. The *Advanced Settings* dialog box opens.



Configure the following settings and then select *Apply*:

Offline Mode	Enabling *Offline Mode* shuts down the protocol used to communicate with managed devices. This is a feature you can use to troubleshoot problems, allowing you to change FortiManager unit settings without affect managed devices.FortiManager cannot automatically connect to FortiGate if offline mode is enabled.

ADOM Mode	Select the ADOM mode, either *Normal* or *Advanced*. Advanced mode will allow you to assign a VDOM from a single device to a different ADOM, but will result in a reduced operation mode and more complicated management scenarios. It is recommended only for advanced users.
Download WSDL file	Select the required WSDL functions and select the *Download* button to download the WSDL file to your management computer. When selecting *Legacy Operations*, no other options can be selected. Web services is a standards-based, platform independent, access method for other hardware and software APIs. The file itself defines the format of commands the FortiManager will accept as well as the response to expect. Using the WSDL file, third-party or custom applications can communicate with the FortiManager unit and operate it or retrieve information just as an administrative user would from the GUI or CLI.
Chassis Management	Enable chassis management, then enter the chassis update interval: 4 to 1440 minutes, default: 15 minutes.
Configuration Changes Received from FortiGate	Select to either automatically accept changes or to prompt the administrator to accept the changes.
Task List Size	Set a limit on the size of the task list.
Verify Installation	Select to preview the installation before proceeding.
Allow Install Interface Policy Only	Select to manage and install interface based policies only instead of all device and policy configuration.

Portal users

You can create external users for use with the FortiManager SDK API. Use the *External Users* tab to add, edit, and delete external users.

To add external users:

1. Go to *System Settings* > *Advanced* > *Portal Users*.
2. Select *Add External User*.
3. Enter the following information, then 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.

Edit an external user:

1. Go to *System Settings* > *Advanced* > *Portal Users*.
2. Select the user from the list and select the edit icon.

3. Edit the password and enabled status.
4. Select *OK* to save the changes.

Delete an external user:

1. Go to *System Settings* > *Advanced* > *Portal Users*.
2. Select the user from the list and select the delete icon.
   A confirmation dialog box is displayed. Select *Yes* to proceed with the delete action.

Restricted Administrator Profiles

In v5.2.0 or later, you can configure restricted administrator profiles. The restricted profile is used by the restricted administrator account. You can use restricted administrator accounts to provide delegated management of Web Filter profiles, Application Sensors, and Intrusion Protection System (IPS) Sensors for a specific ADOM. These restricted administrators can view, edit, and install changes to their ADOM.

To create a custom restricted administrator profile:

1. Go to *System Settings* > *Admin* > *Profile* and select *Create New* in the toolbar. The *Create Profile* dialog box appears.
2. Configure the following settings:

Profile Name		Type a name for this profile.
Description		Type a description for this profile. While not a requirement, a description can help to know what the profiles is for or the levels it is set to.
Type		Select *Restricted Admin*.
Permission		Select to enable permission.
	Web Filter Profile	Select to enable the web filter profile permission.
	Application Sensor	Select to enable the application sensor permission.
	IPS Sensor	Select to enable the IPS sensor permission.

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

Restricted administrator accounts

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

To create a new restricted administrator account:

1. Go to *System Settings* > *Admin* > *Administrator* and select *Create New* in the toolbar. The *New Administrator* page is displayed.
2. Configure the following settings:

User Name	Type the name that this administrator uses to log in. This field is available if you are creating a new administrator account.

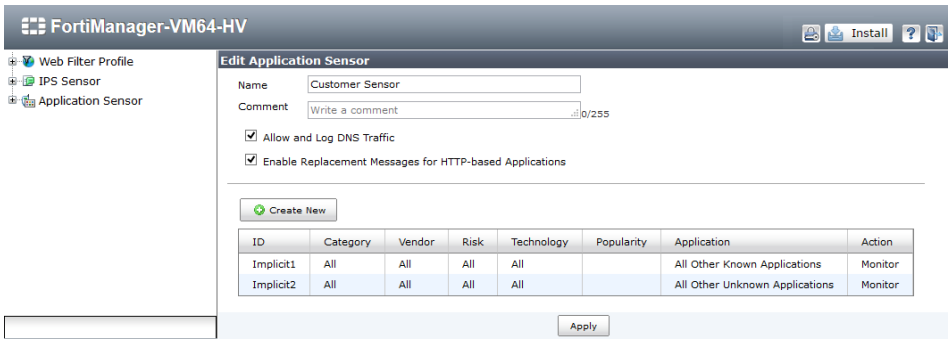
Description	Optionally, type a description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account. (Character limit = 127)
Type	Select the type of authentication the administrator will use when logging into the device. Select one of the following: *LOCAL*, *RADIUS*, *LDAP*, *TACACS+*, or *PKI*.
RADIUS Server	Select the RADIUS server from the drop-down menu. This field is only available when *Type* is set to *RADIUS*.
LDAP Server	Select the LDAP server from the drop-down menu. This field is only available when *Type* is set to *LDAP*.
TACACS+ Server	Select the TACACS+ server from the drop-down menu. This field is only available when *Type* is set to *TACACS+*.
Wildcard	Select to enable wildcard. This field is only available when *Type* is set to *RADIUS*, *LDAP*, or *TACACS+*.
Subject	Type a comment in the subject field for the PKI administrator. This field is only available when *Type* is set to *PKI*.
CA	Select the CA from the drop-down menu. This field is only available when *Type* is set to *PKI*.
Require two-factor authentication	Select to enable two-factor authentication. This field is only available when *Type* is set to *PKI*.
New Password	Type the password. This field is only available when *Type* is set to *LOCAL*, *RADIUS*, *LDAP*, *TACACS+*, or *PKI*.
Confirm Password	Type the password again to confirm it. The passwords must match. This field is only available when *Type* is set to *LOCAL*, *RADIUS*, *LDAP*, *TACACS+*, or *PKI*.
Admin Profile	Select a restricted administrator profile from the drop-down menu. The profile selected determines the administrator's access to the FortiManager unit's features.
Administrative Domain	Choose the ADOMs this administrator will be able to access. This field is only available if ADOMs are enabled.
Web Filter Profile	Select the web filter profile that the administrator will have access to. Select the add icon to add multiple Web Filter profiles.
Application Sensor	Select the Application Sensor that the administrator will have access to. Select the add icon to add multiple Application Sensors.
IPS Sensor	Select the IPS Sensor that the administrator will have access to. Select the add icon to add multiple IPS Sensors.

Trusted Host	Optionally, type the trusted host IPv4 or IPv6 address and netmask that the administrator can log in to the FortiManager unit from. Select the add icon to add trusted hosts. You can specify up to ten 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 86.
User Information (optional)	
Contact Email	Type a contact email address for the new administrator. This email address is also used for workflow session approval email notifications.
Contact Phone	Type a contact phone number for the new administrator.

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

FortiManager portal

When the restricted administrator logs into the FortiManager, they have access to the security profiles that are configured for the account.



The following options are available:

Install	Select to install changes to the ADOM.
Change Password	Select the change password icon in the toolbar to change your account password. A *Change Password* dialog box is displayed. Type your old password, the new password, confirm the password, and select *OK* to save the new password. This option must be enabled via the CLI.
Help	Select the help icon in the toolbar to load the FortiManager online help. The online help will be loaded in a new browser window.
Log Out	Select the log out icon to log out of FortiManager.

Web Filter Profile	When the Web Filter Profile permission is enabled in the restricted administrator profile, this menu will be displayed. The Web Filter Profile selected in the restricted administrator account will be listed. For information on configuring the Web Filter profile, see the FortiOS documentation for the firmware version of the ADOM. The options will vary based on the ADOM version.
IPS Sensor	When the IPS Sensor permission is enabled in the restricted administrator profile, this menu will be displayed. The IPS Sensor selected in the restricted administrator account will be listed. For information on configuring the IPS sensor, see the FortiOS documentation for the firmware version of the ADOM. The options will vary based on the ADOM version.
Application Sensor	When the *Application Sensor* permission is enabled in the restricted administrator profile, this menu will be displayed. The application sensor selected in the restricted administrator account will be listed. For information on configuring the Application Sensor, see the FortiOS documentation for the firmware version of the ADOM. The options will vary based on the ADOM version.

To enable the restricted user to change their own password:

Log into the device command line interface and enter the following CLI command:

```
config system admin profile
   edit <restricted_admin_profile>
      set change-password enable
end
```

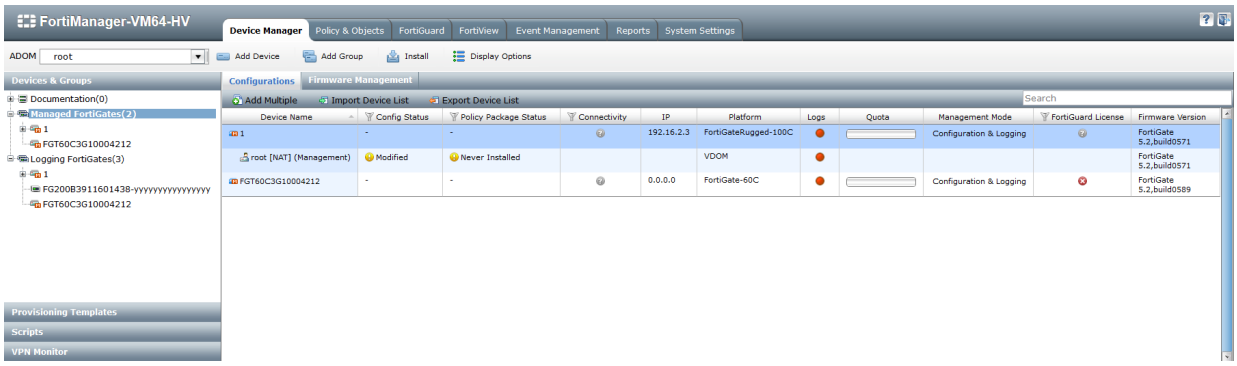
When the restricted administrator logs into their ADOM, the change password icon is displayed in the toolbar.

Device Manager

Use the *Device Manager* tab to view and configure managed devices. This chapter covers navigating the *Device Manager* tab, viewing devices, managing devices, managing FortiAP access points, and managing FortiExtender wireless WAN extenders. For information on adding devices, and installing policy packages see FortiManager Wizards on page 202.

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

The *Device Manager* tab provides access to devices and groups, provisioning templates, scripts, FortiAP, and VPN monitor menus.



The *Device Manager* tab includes the following menus:

Devices & Groups	View and configure managed and logging devices per ADOM. Use the toolbar to add devices, devices groups, and launch the install wizard.
Provisioning Templates	Configure provisioning templates. For information on system, WiFi, Threat Weight, FortiClient, and certificate templates, see Provisioning Templates on page 173.
Scripts	Create new or import scripts. Scripts is disabled by default. You can enable this advanced configuration options in *System Systems* > *Admin* > *Admin Settings*. Select *Show Script* to enable on this option in the *Device Manager* tab tree menu. For more information on scripts, see Scripts on page 218.
FortAP	View and configure managed FortiAP devices.
VPN Monitor	Select VPN Monitor to view Central IPsec and Central SSL-VPN menus. These menus allow you to monitor the VPN connections for the ADOM in a central location. You can also bring up or bring down VPN connections.

Managed/logging device

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

This section contains the following topics:

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

The columns available in Column Settings is dependent on features enabled in FortiManager. When the FortiAnalyzer feature set is disabled, all related settings are hidden in the GUI.

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

Column	Filters
Device Name	Click on the column header to sort the entries in ascending or descending order (alphabetic).
Config Status	Filter by configuration status: • Synchronized • Synchronized from AutoUpdate • Out of Sync • Pending • Warning • Unknown Hover the cursor icon over the column icon for additional information.

Column	Filters
Policy Package Status	Filter by policy package status: • Imported • Installed • Modified • Never Installed • Unknown Hover the cursor icon over the column icon for additional information.
Hostname	Click on the column header to sort the entries in ascending or descending order (alphabetic).
Connectivity	Filter by connectivity status: • Connected • Connection Down • Unknown Hover the cursor icon over the column icon for additional information.
IP	Click on the column header to sort the entries in ascending or descending order (numeric).
Platform	Click on the column header to sort the entries in ascending or descending order (alphabetic).
Logs	Click on the column header to sort the entries in ascending or descending order (log status).
Quota	Click on the column header to sort the entries in ascending or descending order (device log quota). Hover the cursor icon over the column icon for additional information.
Log Connection	Click on the column header to sort the entries in ascending or descending order (log connection status). The log connection can be one of the following states: • IPsec Tunnel is up • IPsec Tunnel is down • IPsec Tunnel is disabled Hover the cursor icon over the column icon for additional information.
FortiGuard License	Filter by license status: • Valid • Expired • Unknown Hover the cursor icon over the column icon for additional information.
Firmware Version	Click on the column header to sort the entries in ascending or descending order (firmware version).

Column	Filters
Description	Click on the column header to sort the entries in ascending or descending order (description). You can left-click the description cell to add a description to the entry. Select *OK* to save the change.
Other	Filter by Description, Contact, City, Province/State, Country, Company/Organization.

View managed/logging devices

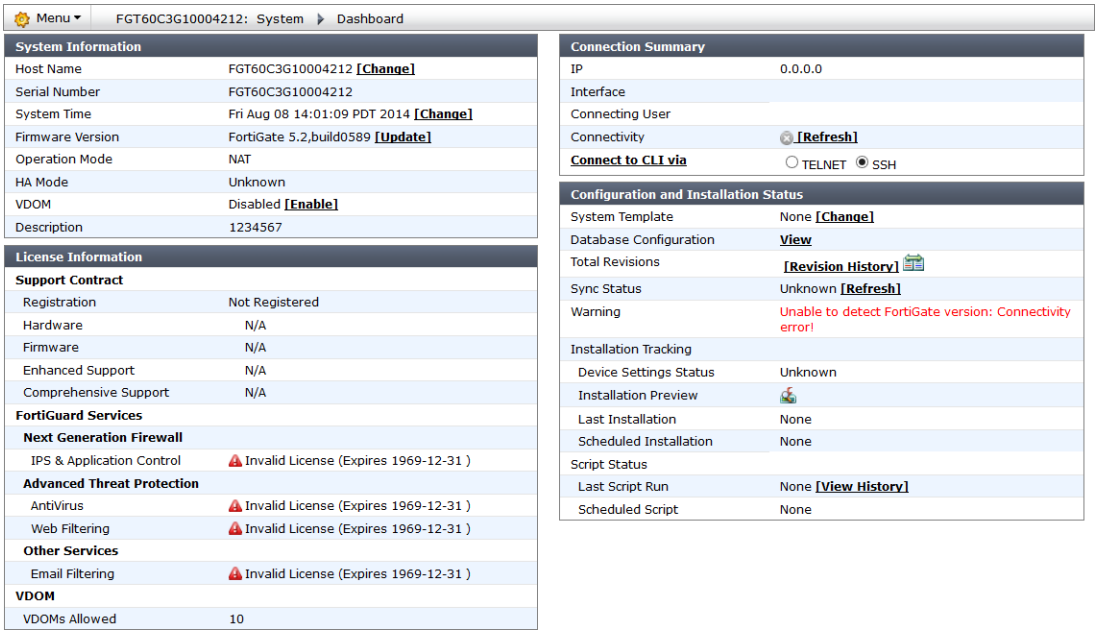
You can view information about individual devices in the *Device Manager* tab. This section describes the FortiGate unit summary.

To view managed/logging devices:

1. Select the *Device Manager* tab.
2. Select the ADOM from the drop-down list.
3. Select the device group, for example *Managed FortiGates,* in the tree menu.

When the FortiAnalyzer feature set is enabled, the *All FortiGates* device group is replaced with *Managed FortiGates* and *Logging FortiGates* . Managed FortiGates include FortiGate devices which are managed by FortiManager but do not send logs. Logging FortiGates include FortiGate devices which are not managed, but do send logs to FortiManager .

4. Select a device or VDOM from the list of managed devices. The device dashboard and related information is shown in the left content pane.



Dashboard toolbar

The dashboard toolbar allows you to select the content, or panel, that is shown in the content pane.

The dashboard toolbar displays the device name and current panel on the right-hand side. Hovering the cursor over the *Menu* drop-down menu, on the left-hand side of the toolbar, will display the available panels organized into categories.

The available panels can be customized at both the ADOM and device levels. Select *Display Options* in the toolbar to open the *Customize Device Tabs* dialog box to customize the available content at the ADOM level. Alternatively, you can select *Menu* > *Customize* to customize device tabs. You can select to inherit from ADOM or customize. Select *[Customize]* in the dashboard toolbar to customize the available panels 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.

To select all of the content panels in a particular category, select *All On* in that categories row. To reset a categories selection, select *Reset*.

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

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

The following options are available in the System category:

Dashboard	View device dashboard widgets including: • *System Information*: View device host name, serial number, update firmware, enable VDOMs, and change system time. • *License Information*: View support contract and other device license information. • *Connection Summary*: Refresh connectivity and connect to the device CLI via TELNET or SSH. • *Configuration and Installation Status*: Change the system template, view database configuration, view revision history and revision diff, refresh sync status, installation preview, and view script history. For more information, see Dashboard widgets on page 137 .
Interface	Configure interfaces, VDOM links, mapping for interfaces, and intra-zone traffic. Select to create a new interface, VDOM link, or virtual WAN.
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 including up to three dialup accounts.
Sniffer Policy	Configure sniffer policies.
HA	View high availability configuration and cluster settings.
SNMP	Create new, enable, disable, and view SNMP v1, v2c, v3 Agent and Community configuration.
DNS	Configure IPv4 and IPv6 DNS or FortiGuard DDNS settings.
DNS Database	Create new, edit, and delete DNS zones.
DNS Service on Interface	Configure the DNS service on the interface. Select the interface from the drop-down list and then select the mode. You can select one of the following modes: *Recursive* , *Non-recursive* , or *Forward to System DNS* .
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, Web Administration Ports, Timeout Settings, Web Administration, and LCD Panel.
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	Import, view, and delete CA certificates.

Replacement Message	Configure replacement messages for the following categories: *Mail*, *HTTP*, *Web Proxy*, *FTP Proxy*, *FTP*, *NNTP*, *Alert Mail*, *Spam*, *Administration*, *Authentication*, *Captive Portal Default*, *FortiGuard Web Filtering*, *IM and P2P*, *Endpoint NAC*, *NAC Quarantine*, *Traffic Quota Control*, *SSL VPN*, and *Security*.
FortiGuard	Configure FortiGuard Distribution Network (FDN) services and settings.
Messaging Servers	Configure SMTP server settings.
Log Setting	Configure logging, and archiving settings. Enable event logging, and specify the types of events to log. You can select to enable memory logging, send logs to FortiAnalyzer/ FortiManager , or Syslog.
Alert E-mail	Configure alert email settings.
NAT64 Prefix	Enable NAT64 prefix and configure NAT64 prefix and always synthesize AAAA records.
Threat Weight	Use the shared threat weight profile or configure a threat weight profile.
FortiSandbox	Enable Sandbox inspection and configure the IP address and notifier email of your FortiSandbox device.

The following options are available in the Router category:

Routing Table	View the routing table.
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.
Multicast Address	Configure multicast addresses.

The following options are available in the Dynamic Objects category:

Address	Configure dynamic to local address mappings.
IPv6 Address	Configure IPv6 dynamic to local address mappings.
Virtual IP	Configure dynamic virtual IP to local virtual IP mappings.
IPv6 Virtual IP	Configure IPv6 dynamic virtual IP to local virtual IP mappings.
NAT46 Virtual IP	Configure NAT64 dynamic virtual IP to local virtual IP mappings.
NAT64 Virtual IP	Configure NAT64 dynamic virtual IP to local virtual IP mappings.
IP Pool	Configure dynamic IP pool to local IP pool mappings.
IPv6 Pool	Configure dynamic IPv6 pool to local IP pool mappings.
Local Certificate	Configure dynamic local certificate to VPN local certificate mappings.
VPN Tunnel	Configure dynamic VPN tunnel to VPN tunnel mappings.
RADIUS Server	Map a dynamic RADIUS server to a local RADIUS server.
Tag Management	Configure Tag Management.

The following options are available in the WAN Opt. & Cache category:

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.
URL Match List	Create, view, edit, and delete URL match entries.
Exempt List	Configure exempt URLs.

The following options are available in the VPN category:

IPsec Phase 1	Configure IPsec Phase 1 settings. Create FortiClient VPN.
IPsec Phase 2	Configure IPsec Phase 2 settings.
Manual Key	Configure manual key settings.

Concentrator	Configure concentrator settings.
SSLVPN Config	Configure SSL VPN settings including DNS and WINS servers.

The following options are available in the Client Reputation Profile category:

Client Reputation Profile	Select to use a shared client reputation profile from the drop-down list or select *Specify* to define the profile.

The following options are available in the User & Device category:

Endpoint Profile	Create, view, edit, and delete FortiClient profiles.
Client Reputation Profile	Create, view, edit, and delete client reputation profiles.

The following options are available in the Wireless category:

Managed FortiAP	Discover and authorize FortiAP devices. View managed FortiAP settings.
WiFi SSID	Configure WiFi SSID.
WIDS Profile	Configure wireless intrusion detection system (WIDS) 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.

The following options are available in the Query category:

DHCP	DHCP query for the selected device.
IPsec VPN	IPsec VPN query for the selected device. You can also change the status of a connection from this tab.
SSL-VPN	SSL-VPN query information for the selected device.
User	User query for the selected device. You also have the option to de-authorize a user.
Session	Session query information for the selected device.
Traffic Shaper	Traffic Shaper query information for the selected device.

FortiToken	FortiToken query for the selected device. You can also activate a FortiToken from this tab.
Web Filter	Web filter query for the selected device.
Application	Application query for the selected device.
Email	Email query for the selected device.
Routing	Routing query for the selected device.
Archive & Data Leak	Archive and data leak queries for the selected device.
WiFi Clients	WiFi client queries.
Rogue AP	Rogue AP queries. You also have the option of changing the status of a connection from this tab.
Logging	Logging queries.

The following option is available in the Report category:

Report	View, download, and delete device reports.

The following options are available at the ADOM level only:

Inherit From ADOM	Select to inherit the customize device tabs settings from the ADOM.
Customize	Select to customize the device tabs settings for the device selected.

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

CLI-Only Objects menu

FortiManager v5.2.0 or later includes an *CLI-Only Objects* menu in the *Device Manager* tab which allows you to configure device settings which are normally configured via the at the CLI on the device. Select the device in the ADOM, and select *Menu* > *CLI-Only Objects* .

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

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 5.0:

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

The following table provide a description of these dashboard widgets. Note that not all of the listed options will be available on every device.

System Information	
Host Name	The name of the device. Select *Change* to change the name.
Serial Number	The device serial number.
System Time	The device system time and date information. Select *Change* to set time or synchronize with NTP server.
Firmware Version	The device firmware version and build number. Select *Update* to view and update the device firmware.
Hardware Status	The number of CPUs and the RAM size.
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 host name, serial number, role, and status of cluster members.
VDOM	The status of VDOMs on the device. Select *Enable/Disable* to change the VDOM role.
Session Information	Select *View Session List* to view the device session information.
Description	Descriptive information about the device.
Operation	Select to *Reboot* or *Shutdown* the managed device.

License Information	
VM License	The VM license status and resources.

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	
System Template	The system template associated with the device. Select *Change* to set this value.
Database Configuration	Select *View* to display the configuration file of the FortiGate unit.
Total Revisions	Displays the total number of configuration revisions and the revision history. Select *Revision History* to view device history. Select the revision history icon to open the *Revision Diff* menu. You can view the diff from a previous revision or a specific revision and select the output.
Sync Status	The synchronization status with the FortiManager. • *Synchronized*: The latest revision is confirmed as running on the device. • *Out_of_sync*: The configuration file on the device is not synchronized with the FortiManager system. • *Unknown*: The FortiManager system is unable to detect which revision (in revision history) is currently running on the device. Select *Refresh* to update the Installation Status.

Configuration and 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 the icon to display a set of commands that will be used in an actual device configuration installation in a new window.
Last Installation	*Last Installation*: The FortiManager system sent a configuration to the device at the time and date listed.
Scheduled Installation	*Scheduled Installation*: A new configuration will be installed on the device at the date and time indicated.
Script Status	Select Configure to view script execution history.
Last Script Run	Displays the date when the last script was run against the managed device.
Scheduled Script	Displays the date when the next script is scheduled to run against the managed device.

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

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 v5.2/v5.0 devices into one ADOM, and all v4.3 into another.
- Geographic regions: group all devices for a specific geographic region into an ADOM, and devices for a separate region into another ADOM.

- Administrator users: group devices into separate ADOMs based for specific administrators responsible for the group of devices.
- Customers: group all devices for one customer into an ADOM, and devices for another customer into another ADOM.

  FortiMail, FortiWeb, FortiSwitch, FortiCache, FortiSandbox, Chassis, and FortiCarrier devices are automatically placed in their own ADOMs.

Each administrator profile can be customized to provide read-only, read/write, or restrict access to various ADOM settings. When creating new administrator accounts, you can restrict which ADOMs the administrator can access, for enhanced control of your administrator users. For more information on ADOM configuration and settings, see Administrative Domains on page 32 .

For information on adding devices to an ADOM using the *Add Device* wizard, see FortiManager Wizards on page 202.

Device groups

Device groups can be added, deleted, and edited as required to assist you in organized your managed devices. The firmware of the devices within a group can also be updated as a group.

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.
2. Complete the following fields:

Group Name	Type 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	Type 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.

Device groups can also be added from the *Task Monitor*. See for more Task monitor on page 105 information.

To edit a 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.

To update device group firmware:

1. Right-click on a device group in the tree menu and select *Firmware Update* under the *Device Group* heading in the right-click menu. The *Group Firmware Information* screen opens.
2. Locate an applicable firmware image inthe Available Upgrade list, then select *Upgrade* to upgrade all of the devices in the group to that image.

   The upgrade history is also shown, and can be viewed in more detail by selecting the *All History* icon.
3. Select *Return* to return to the group screen.

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 in the *Device Manager* tab, the configuration is available within other tabs in the FortiManager system including *Policy & Objects* , Log View, Event Management, 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
- Re-install Policy
- Importing and exporting device lists

- Setting unregistered device options
- Firmware Management

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. Type 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. Select the ADOM from the drop-down list.
2. Select the *Add Device* icon in the toolbar. The *Add Device* wizard opens.
3. Select *Discover* for a device which is online. Select *Add Model Device* to provision a device which is not yet online.
4. 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 202.

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 al devices that are being managed by your FortiManager, use the following command:

```
diagnose dvm device list
```

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

Changing the serial number from the CLI

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

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

This command is also useful when performing an RMA replacement.

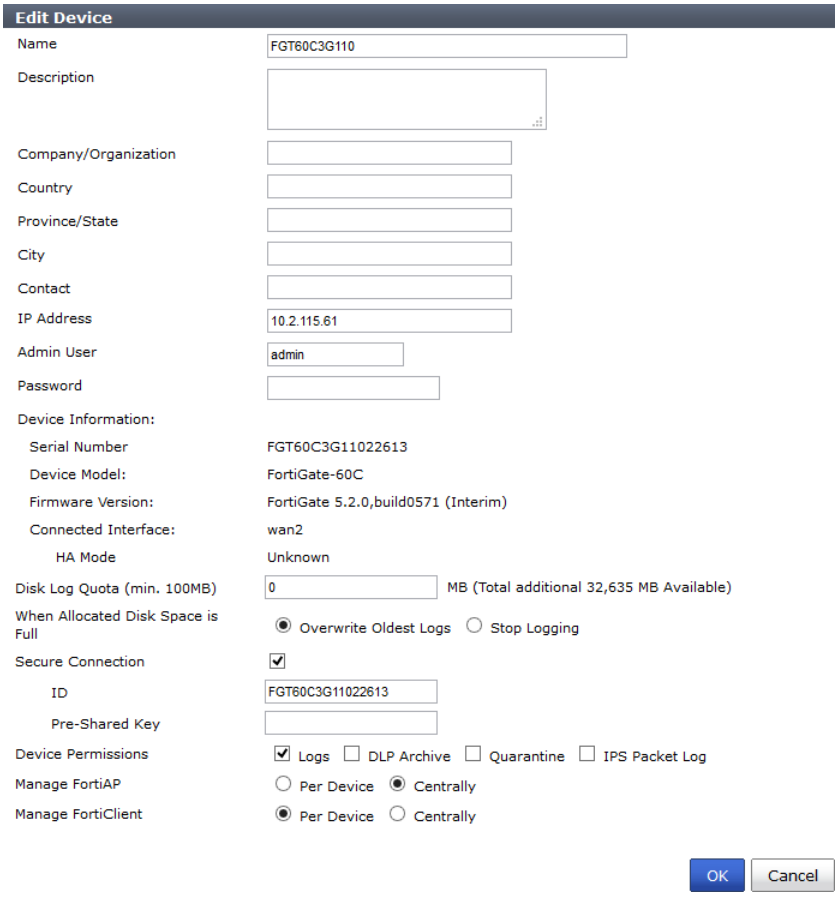
Editing device information

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

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

To edit information for a single device:

1. Select the ADOM from the drop-down list.
2. In the tree menu select the device group and device.
3. Right-click on the device row and select *Edit* from the right-click context menu.



4. Edit the following settings as required.

Name	The name of the device.
Description	Descriptive information about the device.
Company /Organization	Company or organization information.

Country	Type the country.
Province/State	Type the province or state.
City	Type the city.
Contact	Type the contact name.
IP Address	The IP address of the device.
Admin User	The administrator user name.
Password	The administrator 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. The minimum value is 100MB. The maximum value depends on the device model and available disk space. This field is only available when *FortiAnalyzer Features* is enabled.
When Allocated Disk Space is Full	The action for the system to take when the disk log quota is filled. This field is only available when *FortiAnalyzer Features* is enabled.
Secure Connection	Select check box to enable this feature. Secure Connection secures OFTP traffic through an IPsec tunnel. This field is only available when *FortiAnalyzer Features* is enabled. Enter the device serial number in the *ID* field, and the The pre-shared key for the IPsec connection between the FortiGate and FortiManager in the *Pre-Shared Key* field.
Device Permissions	The device's permissions. Device permissions include: *Logs*, *DLP Archive*, *Quarantine*, and *IPS Packet Log*. This field is only available when *FortiAnalyzer Features* is enabled.
Manage FortiAP	Select to manage FortiAP per device or centrally. When managing FortiAP centrally, FortiAP devices will be listed in the *All FortiAP* group in the ADOM. When selecting to manage FortiAP per device, you will select the FortiGate that is managing the FortiAP and select the *System* > *FortiAP* device tab. You can configure WiFi templates in the *Provisioning Templates* > *WiFi Templates* > *Custom AP Profiles* section.
Manage FortiClient	Select to manage FortiClient per device or centrally. You can configure FortiClient templates in the *Provisioning Templates* > *FortiClient Templates* > *FortiClient Profile* section.

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

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

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

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

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.
2. Select *Refresh* from the pop-up menu. The *Update Device* dialog box will open to show the refresh progress.
3. You can also select *Refresh* on the *Connection Summary* widget by selecting *[Refresh]* in the *Connectivity* field.

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. Select the ADOM from the drop-down list.
2. Select *Install* in the toolbar. The *Install Wizard* will appear.
3. 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.
4. 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 202 .

Re-install Policy

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

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.

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

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

There are two ways to create the text file:

- Export the 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 151 .

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 150 .

Field	Blank Allowed	Description
name	No	Name of the ADOM.
mode	No	In FortiManager 5.0 the mode is GMS. This field reflects legacy code.
status	No	Type 1 to enable the ADOM. Type 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 5.0 the value is 0. This field reflects legacy code.
enable	No	Type 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* or 5.2 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|branc
    h_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 user name.
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.

Field Name	Blank Allowed	Description
desc	Yes	Device description.
discover	No	Type 1 to automatically discover device, 0 otherwise.
reload	No	Type 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	Type 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 150), 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.

Field Name	Blank Allowed	Description
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.

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.

```
+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.

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|
```

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

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

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

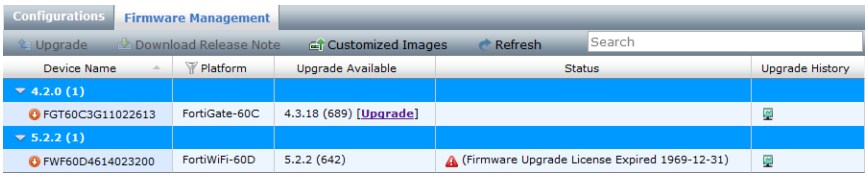
When the `set allow register` command is set to `disable`, you will not receive the following unregistered device dialog box.

Firmware Management

FortiGate device firmware can be updated from the *Firmware Management* tab. Upgrades can also be scheduled to occur at a later date.

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

In the *Device Manager* tab, select an ADOM, select the *Managed FortiGates* group, then select the *Firmware Management* tab.

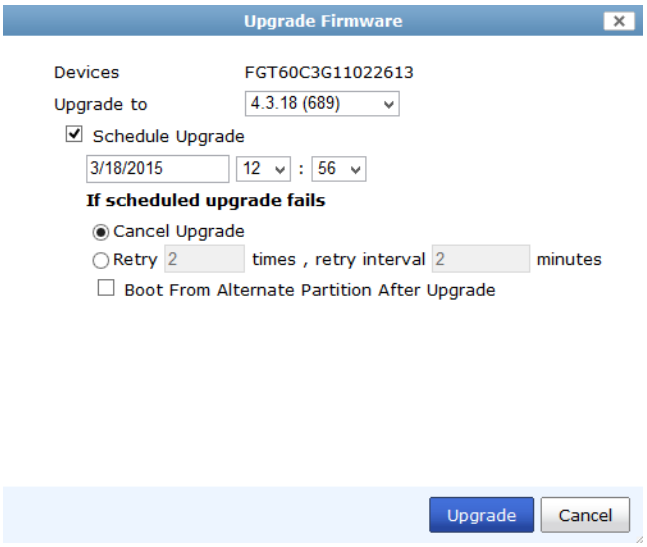


The following information and options are available:

Upgrade	Select to upgrade the selected device if the device can be upgraded.
Download Release Notes	Select to download the release notes for the FortiOS version of the selected device.
Customized Images	Select to go to the customized images page, where you can import or delete images.
Refresh	Refresh the list.
Device Name	The names of the FortiGate devices in the group, organized by firmware version.
Platform	The device platform.
Upgrade Available	The current firmware version and build number of the firmware on the device. If an update is available and can be applied to the device, Upgrade can be selected to open the *Upgrade Firmware* dialog box.
Status	The status of the device's license. If the license has expired, the firmware cannot be upgraded.
Upgrade History	Select the icon to view the device's upgrade history in a dialog box.

To upgrade a device's firmware:

1. In the *Firmware Management* screen, select a device or device group with an upgrade available that is licensed for firmware upgrades, then select *Upgrade* in either the toolbar or in the *Upgrade Available* column. The *Upgrade Firmware* dialog box opens.



2. Configure the following settings:

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

3. Select *Upgrade* to update the device.

Configuring devices

You can configure the FortiGate units in three ways:

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

This section contains the following topics:

Configuring a device

Configuring a FortiGate unit using the *Device Manager* dashboard toolbar is very similar to configuring FortiGate units using the FortiGate GUI. You can also save the configuration changes to the configuration repository and install them to other FortiGate units at the same time.

This document does not provide detailed procedures for configuring FortiGate units. See the FortiGate documentation for complete information. The most up-to-date FortiGate documentation is also available in the Fortinet Document Library .

To configure a FortiGate unit:

1. In the *Device Manager* tab, select the ADOM from the drop-down list.
2. Select the unit you want to configure on the tree menu.
3. Select an option for that unit in the dashboard toolbar.
4. Configure the unit as required.

   The configuration changes are saved to the FortiManager device database instead of the FortiManager repository represented by the *RevisionHistory* window.

You can rename and reapply firewall objects after they are created and applied to a firewall policy. When you do so, the FortiManager system will: delete all dependencies, delete the object, recreate a new object with the same value, and recreate the policy to reapply the new object.

Firewall policy reordering on first installation

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

This behavior is normal for the following reasons:

- The FortiManager system maintains the order of policies in the actual order you see them and manipulate them in the GUI, whereas the FortiGate unit maintains the policies in a different order (such as order of creation).
- When loading the policy set, the FortiManager system re-organizes the policies according to the logical order as they are shown in the user interface. In other words, FortiManager will group all policies that are organized within interface pairs (internal -> external, port1 -> port3, etc.).

The FortiManager system does not move policies within interface pairs. It will only move the configuration elements so that policies with the same source/destination interface pairs are grouped together.

This behavior would only be seen:

- On the first installation.
- When the unit is first discovered by the FortiManager system. If using the FortiManager system to manage the FortiGate unit from the start, you will not observe the policy reordering behavior.

Out-of-Sync device

FortiManager is able to detect when the settings were changed on the FortiGate and synchronize back to the related policy and object settings. This allows you to know when the policy package is out-of-sync with what is

installed on the FortiGate.

When a change is made to the FortiGate, FortiManager displays an out-of-sync dialog box.

Select the *View Diff* icon to view the changes between the FortiGate and FortiManager .

You can select to accept, revert the modification, or decide later.

When accepting remote changes, all local configurations will be replaced by remote configurations. When reverting, the FortiGate will be reset to the latest revision.

You can view details of the retrieve device configuration action in the Task Manager.

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 FortiOS Handbook available in the Fortinet Document Library .

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

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

Creating and editing virtual domains

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

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

To enable virtual domains:

1. In the *Device Manager* tab, select the unit you want to configure.
2. In 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 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 content pane tab bar. See Managed/logging device on page 129 for more information.

3. After the first VDOM is created you can create additional VDOMs by right-clicking on the existing VDOM and selecting *Add VDOM* from the right-click menu.
4. Type the name, operation mode and an optional description for the new VDOM. If you selected Transparent mode, you also need to type the management IP address and netmask, as well as the gateway.
5. Select *Submit* to create the new VDOM.

Configuring inter-VDOM routing

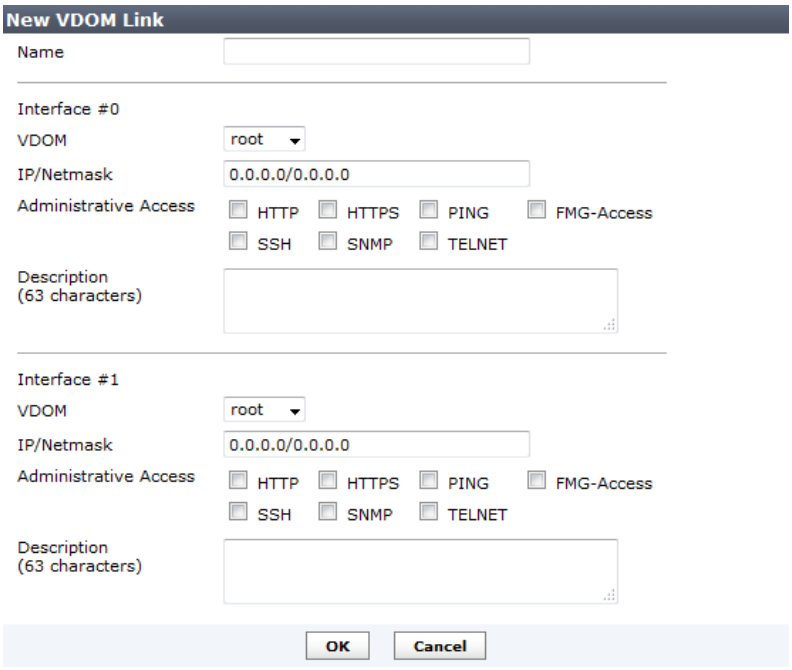
By default, for two virtual domains to communicate it must be through externally connected physical interfaces. Inter-VDOM routing creates a link with two ends that act as virtual interfaces, internally connecting the two virtual domains.

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 *Interface* device tab.
3. Select *Create New* > *VDOM Link* from the toolbar. The *New VDOM Link* window opens.



4. Enter the following information:

Name	Name of the VDOM link.
Interface #x	The interface number, either *1* or *0*.
VDOM	Select the VDOM
IP/Netmask	Type the IP address and netmask for the VDOM.
Administrative Access	Select the allowed administrative service protocols from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, and Web Service.
Description	Optionally, type a description for the link.

5. 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.

To configure a VDOM's resource limits:

1. In the *Device Manager* tab, select the unit you want to configure.
2. Select the *Virtual Domain* tab in the content pane, then select the *Resource* icon for one of the VDOMs in the list. The *Resource Usage* page opens.
3. For each resource:
   - type the maximum value allowed for this resource. If you type a wrong value, a warning appears with the correct value range.
   - type 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 content pane, select the *Global Resources* tab.
   The following information and option is available:

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.
Select All	Right-click, select *Select All* , and select *Reset* to reset all global resources.

FortiAP

You can select to manage FortiAPs per device or centrally in the *Edit Device* page. When managing FortiAP centrally, FortiAP devices will be listed in the *All FortiAP* group, in the *FortiAP* tree menu, in the ADOM. The right-click menu includes options to assign a profile, create new, edit, delete, authorize, deauthorize, upgrade, restart, refresh, view clients, and view rogue APs. The *All FortiAP* group contains thin access points (FortiAP) and thick access points (FortiWiFi).

When selecting to manage FortiAP per device, you will select the FortiGate that is managing the FortiAP and select the *System* > *FortiAP* device tab.

To view the list of FortiAP/FortiWiFi access points, in the *Device Manager* tab, select desired ADOM, then select *All FortiAP*. The FortiAP list is shown in the content pane. The following information is provided:

FortiGate	The FortiGate that is managing the FortiAP/FortiWiFi access point. Click the column header to sort the entries in ascending or descending order.
VDOM	The VDOM that contains the FortiAP/FortiWiFi access point.
Access Point	The access point. Click the column header to sort the entries in ascending or descending order.
Model	The device model. Click the column header to sort the entries in ascending or descending order.
Serial Number	The device's serial number. Click the column header to sort the entries in ascending or descending order.
State	The state of the FortiAP/FortiWiFi access point. Hover the cursor over the icon to see a description of the state. Click the column header to sort the entries in ascending or descending order.
Connected Via	The method by which the device is connected to the FortiGate.
AP Profile	The AP Profile assigned to the device. Click the column header to sort the entries in ascending or descending order.
Join Time	The time that the device joined.
Channel	The channel or channels used by the device.
OS Version	The operating system version running on the device.
SSIDs	The SSIDs associated with the access point.

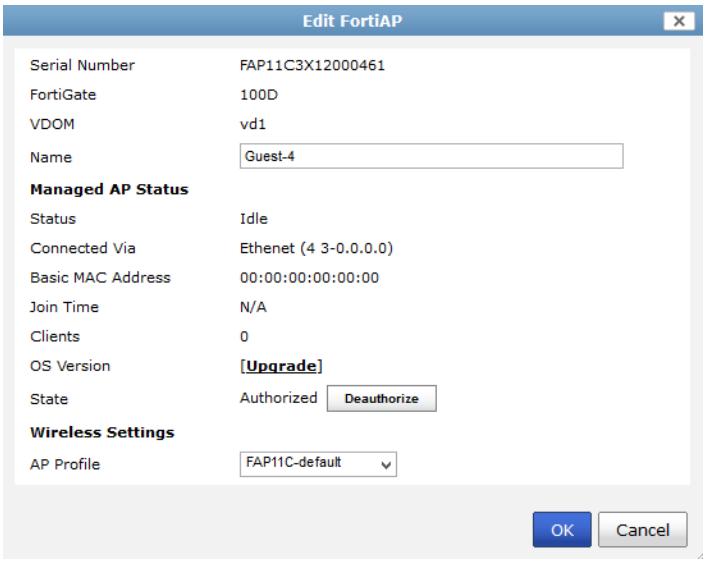
Select *Column Settings* from the toolbar to edit columns and the order they are displayed.

To add a FortiAP/FortiWiFi access point:

1. In the All FortiAP group, right-click on a device and select *Create New* from the pop-up menu. The *Edit FortiAP* dialog box is displayed.
2. Type the FortiAP serial number, the name, and select OK.
   The new FortiAP will auto install to FortiGate. The number of FortiAPs that can be installed is dependent on the FortiGate model.

To edit a FortiAP/FortiWiFi access point:

1. In the All FortiAP group, right-click on a device and select *Edit* from the pop-up menu, or simply select the device's serial number. The *Edit FortiAP* dialog box opens.



2. Configure the following settings:

Serial Number	The device's serial number. This field cannot be edited.
FortiGate	The FortiGate that is managing the device. This field cannot be edited.
VDOM	The VDOM that contains the FortiAP/FortiWiFi access point. This field cannot be edited.
Name	Type a name for the FortiAP/FortiWiFi access point.
Managed AP Status	
Status	The status of the FortiAP/FortiWiFi access point, such as *Connected* . This field cannot be edited.
Connected Via	The method by which the device is connected to the FortiGate. This field cannot be edited.
Basic MAC Address	The MAC address of the device. This field cannot be edited.
Join Time	The time that the device joined. This field cannot be edited.
Clients	The number of clients connected to the device. This field cannot be edited.
OS Version	The operating system version being used by the device. This field cannot be edited.
State	Select *Authorize* or *Deauthorize* to authorize or deauthorize the device.
Wireless Settings	
AP Profile	Select an AP profile to apply to the device from the drop-down list. The list will be limited to profiles that correspond to the device model.

3. Select *OK* to save your changes.

To authorize a discovered FortiAP device:

1. In the All FortiAP group, right-click on a device and select *Authorize* from the pop-up menu. Optionally, you can select *Edit* from the pop-up menu and select to authorize the device in the *Edit FortiAP* dialog box. A dialog box will be displayed with the authorization status.
2. Select *OK* to close the dialog box.

To deauthorize an access point:

1. In the All FortiAP group, right-click on a device and select *Deauthorize* from the pop-up menu. Optionally, you can select *Edit* from the pop-up menu and select to deauthorize the device in the *Edit FortiAP* dialog box. A dialog box will be displayed with the authorization status.
2. Select *OK* to close the dialog box.

To assign a profile to an access point:

In the All FortiAP group, right-click on a device, select *Assign Profile* from the pop-up menu, and select an available AP profile. Optionally, you can select *Edit* from the pop-up menu and select to deauthorize the device in the *Edit FortiAP* dialog box.

To restart an access point:

In the *All FortiAP* group, right-click on a device and select *Restart* from the pop-up menu.

To update the FortiAP device firmware:

1. Right-click on a device in the FortiAP list and select *Upgrade* from the pop-up menu. Optionally, you can select *Edit* from the pop-up menu and select to upgrade the device in the *Edit FortiAP* dialog box.

   The *Upgrade Firmware* dialog box opens, listing the available updates.
2. Select *Upgrade Now* , and then select *OK* in the confirmation dialog box, to update the FortiAP to the selected firmware version.

FortiAP clients

To view the FortiAP client list, right-click on a device in the FortiAP list and select *View Clients* from the pop-up menu. The FortiAP client list dialog box opens, displaying the following information:

IP	The device IP address. Click the column header to sort the entries in ascending or descending order.
FortiAP	The device serial number. Click the column header to sort the entries in ascending or descending order.
Name	The SSID name used by the device. Click the column header to sort the entries in ascending or descending order.
MAC Address	The device's MAC address. Click the column header to sort the entries in ascending or descending order.

Auth	The device's authentication. Click the column header to sort the entries in ascending or descending order.
Vendor Info	The device vendor information. Click the column header to sort the entries in ascending or descending order.
Rate	The transfer rate of the device. Click the column header to sort the entries in ascending or descending order.
Signal Strength	The signal strength provided by the device. Click the column header to sort the entries in ascending or descending order.
Idle Time	The amount of time the device has been idle. Click the column header to sort the entries in ascending or descending order.
Association Time	The time the device has been associated. Click the column header to sort the entries in ascending or descending order.
Bandwidth Tx/Rx	The available bandwidth. Click the column header to sort the entries in ascending or descending order.

A search field is available to allow you search clients listed in the pop-up dialog box.

Rogue APs

To view the rogue AP list, right-click on a device in the FortiAP list and select *View Rogue APs* from the pop-up menu. The *Rogue AP* dialog box opens. The information in the list can be sorted by column by selecting the column heading.

The following information is shown:

State	The state of the device, if known.
Online Status	The status of the device: whether or not it is online.
SSID	The SSID used by the device.
MAC Address	The device's MAC address.
Vendor Info	The device vendor information.
Security Type	The type of security used by the device.
Signal Strength	The signal strength of the device.
Channel	The channel being used by the device.
Rate	The rate of the device.

First Seen	The time the device was first seen.
Last Seen	The time the device was last seen.
Directed By	The device directing the rogue AP.
On-Wire	If the device is on-wire.
Page controls	Scroll through the various pages of rogue AP listings.

FortiExtender

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

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

Centrally managed

When managing FortiExtender centrally, FortiAP devices will be listed in the *All FortiExtender* group in the ADOM of the FortiGate managing the FortiExtender.

The following information is displayed:

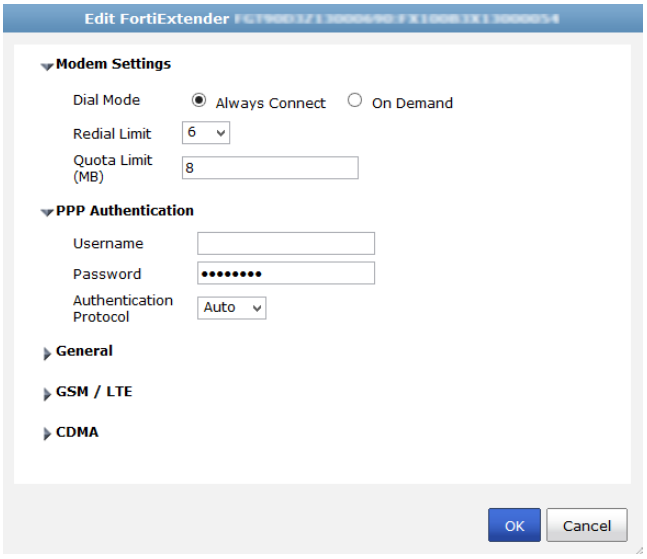
Device Name	The serial number of the FortiGate device that is managing the FortiExtender.
Serial Number	The serial number of the FortiExtender.
Priority	The FortiExtender priority, either *Primary* or *Secondary*.
Model	The FortiExtender model.
Management Status	The FortiExtender management status, either *Authorized* or *Deauthorized*.
Status	The FortiExtender status, either *Up* or *Down*.
Network	The FortiExtender network status and carrier name.
Current Usage	The current data usage.
Last Month Usage	The data usage for the last month.
Version	The FortiExtender firmware version.

The right-click menu options include:

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

To edit a FortiExtender:

1. Go to *Device Manager* > *All FortiExtender* .
2. Select the FortiExtender from the list, right-click, and select *Edit* in the menu. The *Edit FortiExtender* page is displayed.



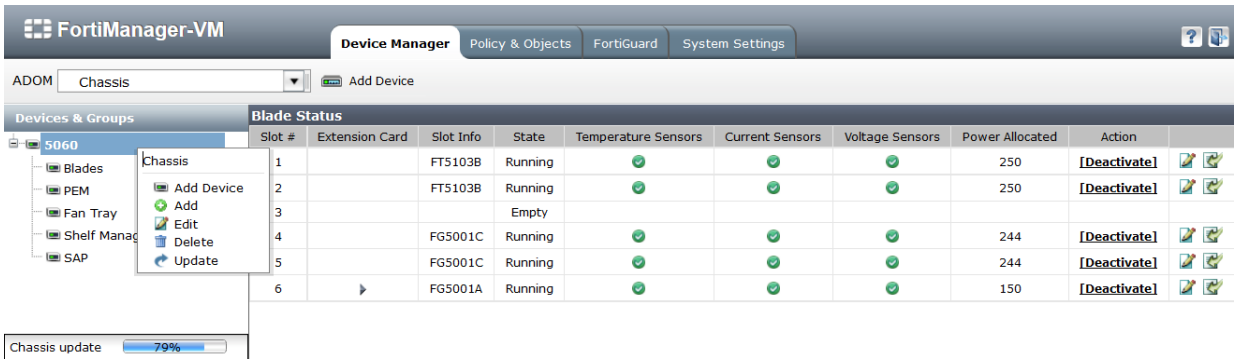
3. Configure the following settings:

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

4. Select *OK* to save the setting.

FortiGate chassis devices

Select FortiManager systems can work with the Shelf Manager to manage FortiGate 5050, 5060, 5140, and 5140B chassis. The Shelf Manager runs on the Shelf Management Mezzanine hardware platform included with the FortiGate 5050, 5060, 5140, and 5140B chassis. You can install up to five FortiGate 5000 series blades in the five slots of the FortiGate 5050 ATCA chassis and up to 14 FortiGate 5000 series blades in the 14 slots of the FortiGate 5140 ATCA chassis. For more information on FortiGate 5000 series including Chassis and Shelf manager, see the Fortinet Document Library.



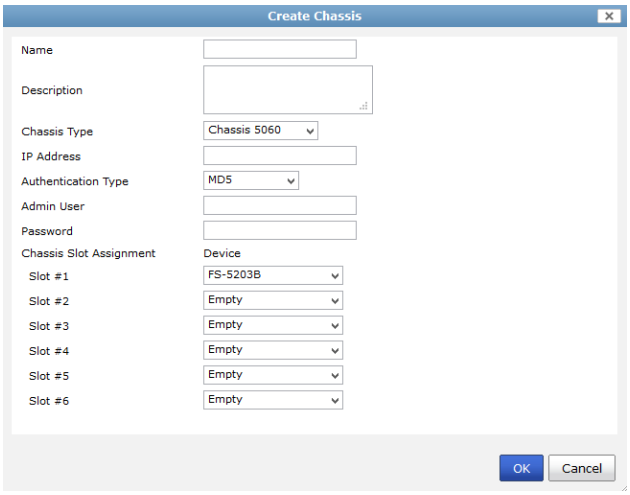
You need to enable chassis management before you can work with the Shelf Manager through the FortiManager system.

To enable chassis management:

1. In the *System Settings* tab, go to *System Settings* > *Advanced* > *Advanced Settings*. See Advanced settings on page 121 for more information.
2. Under *Advanced Settings*, select *Chassis Management* .
3. Set the *Chassis Update Interval*, from 4 to 1440 minutes.

To add a chassis:

1. In the *Device Manager* tab, right-click in the tree menu and select *Chassis* > *Add* . The *Create Chassis* window opens.



2. Complete the following fields:

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

3. Select *OK*.

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

1. In the *Device Manager* tab, right-click the chassis you want to edit and select *Edit* from the pop-up menu.
2. Modify the fields except *Chassis Type* , as required.
3. 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.

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

The following is displayed:

Refresh	Select to update the current page. If there are no entries, Refresh is not displayed.
Slot #	The slot number in the chassis. The FortiGate 5050 chassis contains five slots numbered 1 to 5. The FortiGate 5060 chassis contains six slots numbered 1 to 6. The FortiGate 5140 and 5140B chassis contains fourteen slots numbered 1 to 14.
Extension Card	If there is an extension card installed in the blade, this column displays an arrow you can select to expand the display. The expanded display shows details about the extension card as well as the blade.
Slot Info	Indicates whether the slot contains a node card (for example, a FortiGate 5001SX blade) or a switch card (for example, a FortiSwitch 5003 blade) or is empty.
State	Indicates whether the card in the slot is installed or running, or if the slot is empty.
Temperature Sensors	Indicates if the temperature sensors for the blade in each slot are detecting a temperature within an acceptable range. *OK* indicates that all monitored temperatures are within acceptable ranges. *Critical* indicates that a monitored temperature is too high (usually about 75°C or higher) or too low (below 10°C).
Current Sensors	Indicates if the current sensors for the blade in each slot are detecting a current within an acceptable range. *OK* indicates that all monitored currents are within acceptable ranges. *Critical* indicates that a monitored current is too high or too low.
Voltage Sensors	Indicates if the voltage sensors for the blade in each slot are detecting a voltage within an acceptable range. *OK* indicates that all monitored voltages are within acceptable ranges. *Critical* indicates that a monitored voltage is too high or too low.
Power Allocated	Indicates the amount of power allocated to each blade in the slot.

Action	Select *Activate* to turn the state of a blade from *Installed* into *Running*. Select *Deactivate* to turn the state of a blade from *Running* into *Installed*.
Edit	Select to view the detailed information on the voltage and temperature of a slot, including sensors, status, and state. You can also edit some voltage and temperature values.
Update	Select to update the slot.

To edit voltage and temperature values:

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

Viewing the status of the power entry modules

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

The following is displayed:

Refresh	Select to update the current page.
PEM	The order numbers of the PEM in the chassis.
Presence	Indicates whether the PEM is present or absent.
Temperature	The temperature of the PEM.
Temperature State	Indicates whether the temperature of the PEM is in the acceptable range. *OK* indicates that the temperature is within acceptable range.
Threshold	PEM temperature thresholds.
Feed -48V	Number of PEM fuses. There are four pairs per PEM.
Status	PEM fuse status: present or absent.
Power Feed	The power feed for each pair of fuses.
Maximum External Current	Maximum external current for each pair of fuses.

Maximum Internal Current	Maximum internal current for each pair of fuses.
Minimum Voltage	Minimum voltage for each pair of fuses.
Power Available	Available power for each pair of fuses.
Power Allocated	Power allocated to each pair of fuses.
Used By	The slot that uses the power.

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

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

The following is displayed:

Refresh	Select to update the current page.
Thresholds	Displays the fan tray thresholds.
Fan Tray	The order numbers of the fan trays in the chassis.
Model	The fan tray model.
24V Bus	Status of the 24V Bus: present or absent.
-48V Bus A	Status of the -48V Bus A: present or absent.
-48V Bus B	Status of the -48V Bus B: present or absent.
Power Allocated	Power allocated to each fan tray.
Fans	Fans in each fan tray.
Status	The fan status. *OK* means it is working normally.
Speed	The fan speed.

Viewing shelf manager status

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

The following is displayed:

Refresh	Select to update the current page.
Shelf Manager	The order numbers of the shelf managers in the chassis.
Model	The shelf manager model.

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

Viewing shelf alarm panel (SAP) status

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

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

The following is displayed:

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

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.

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

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

Provisioning Templates

The *Provisioning Templates* section of the *Device Manager* tree menu provides configuration options for the following templates:

- System templates
- WiFi templates
- Threat Weight templates
- FortiClient templates
- Certificate templates

Select the ADOM from the drop-down list then select *Provisioning Templates* in the tree menu.

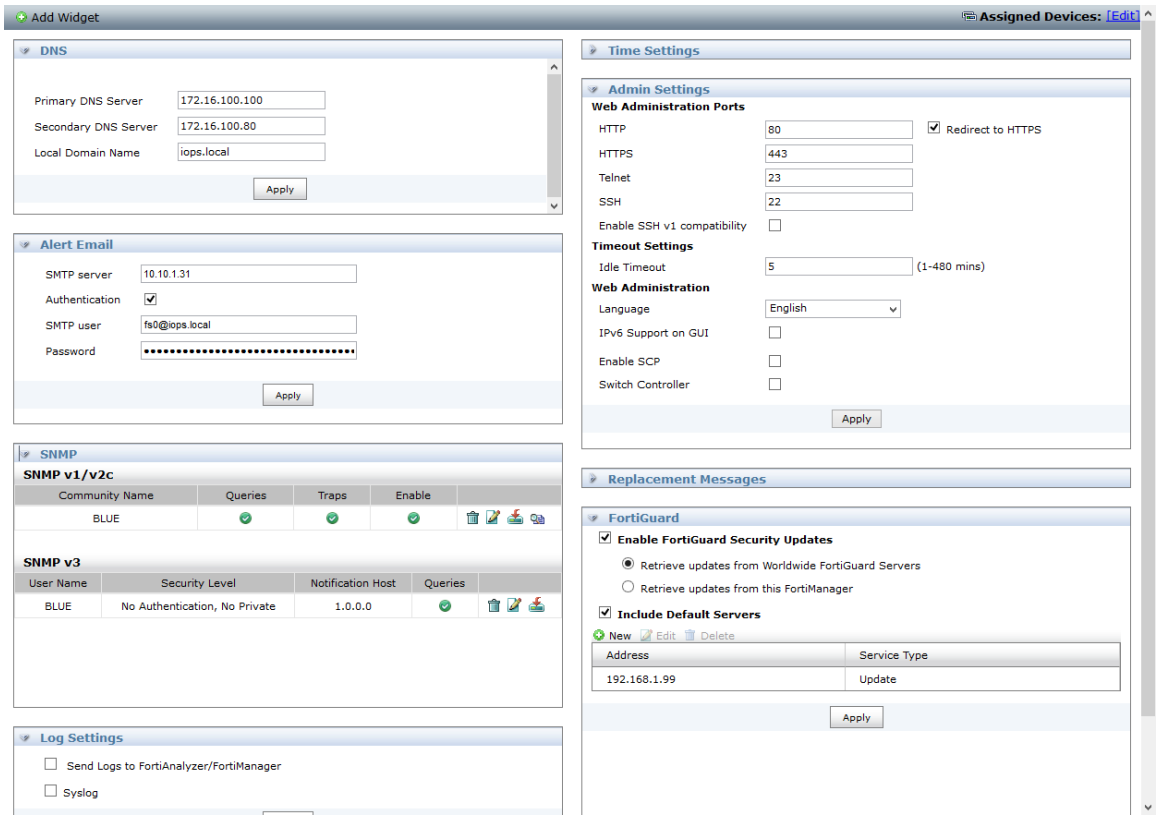
System templates

The *System Templates* menu allows you to create and manage device profiles. A system template is a subset of a model device configuration. Each device or device group will be able to be linked with a system template. When linked, the selected settings will come from the template, not from the Device Manager database.

By default, there is one generic profile defined. System templates are managed in a similar manner to policy packages. You can use the context menus to create new device profiles. You can configure settings in the widget or import settings from a specific device.

Go to the *Device Manager* tab, then select *Provisioning Templates* > *System Templates* > *default* in the tree menu to configure system templates.

System templates are available in v4.3, v5.0, and v5.2 ADOMs. Some settings may not be available in all ADOM versions.



The following widgets and settings are available:

Widget	Description
DNS	Primary DNS Server, Secondary DNS Server, Local Domain Name, IPv6 DNS settings. Configure in the system template or import settings from a specific device. Select *Apply* to save the setting. Hover over the widget heading to select the following options: • Import: Import DNS settings from a specific device. Select the device in the drop-down list. Select *OK* to import settings. Select *Apply* to save the settings. • Refresh: Refresh the information displayed in the widget. • Close: Close the widget and remove it from the system template.

Widget	Description
Time Settings	Synchronize with NTP Server and Sync Interval settings. You can select to use the FortiGuard server or specify a custom server. Configure in the system template or import settings from a specific device. Select *Apply* to save the setting. Hover over the widget heading to select the following options: • Import: Import time settings from a specific device. Select the device in the drop-down list. Select *OK* to import settings. Select *Apply* to save the settings. • Refresh: Refresh the information displayed in the widget. • Close: Close the widget and remove it from the system template.
Alert Email	SMTP Server settings including server, authentication, SMTP user, and password. Configure in the system template or import settings from a specific device. Select *Apply* to save the setting. Hover over the widget heading to select the following options: • Import: Import alert email settings from a specific device. Select the device in the drop-down list. Select *OK* to import settings. Select *Apply* to save the settings. • Refresh: Refresh the information displayed in the widget. • Close: Close the widget and remove it from the system template.
Admin Settings	Web Administration Ports, Timeout Settings, and Web Administration. Configure in the system template and select *Apply* to save the setting. Hover over the widget heading to select the following options: • Refresh: Refresh the information displayed in the widget. • Close: Close the widget and remove it from the system template.
SNMP	SNMP v1/v2 and SNMP v3 settings. SNMP v1/2c: In the toolbar, you can select to delete the record, edit, copy global object, or query object usage. SNMP v3: In the toolbar, you can select to delete the record, edit, or copy global object. Configure in the system template or import settings from a specific device. Select *Apply* to save the setting. Hover over the widget heading to select the following options: • Import: Import SNMP settings from a specific device. Select to import either SNMP v1/v2c or SNMP v3. Select the device in the drop-down list and the objects. Select *OK* to import settings. Select *Apply* to save the settings. • Create New: Create a new SNMP v1/v2c or SNMP v3 community. Type a community name, specify hosts, queries, traps, and SNMP events. Select *OK* to save the setting. • Refresh: Refresh the information displayed in the widget. • Close: Close the widget and remove it from the system template.

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

You can create, edit, or delete profiles by right-clicking on a profile name in the *Provisioning Templates* tree menu under the *System Templates* heading. You can also select the devices that will be associated with the profile by selecting *Assigned Devices* from the right-click menu, or selecting *Edit* from the *Assigned Devices* field in the top right corner of the content pane. A provisioning profile can also be created from a device by selecting *Create From Device* in the right-click menu.

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

WiFi templates

The *WiFi Templates* menu allows you to create and manage SSIDs, Custom AP Profiles, and WIDS Profiles that can be applied to managed FortiAP devices.

WiFi templates are available in v5.0 and v5.2 ADOMs only. Some settings may not be available in all ADOM versions.

SSIDs

To view a list of SSIDs, in the *Provisioning Templates* tree menu, select an ADOM, then select *WiFi Templates* > *SSIDs*.

SSIDs can be created, edited, cloned, deleted, searched, and imported.

The following information is available:

Name	The name given to the SSID.
SSID	The SSID name that is broadcast.
Traffic Mode	The traffic mode for the SSID; one of: • *Tunnel to Wireless Controller*: Data for WLAN passes through the WiFi controller. • *Local bridge with FortiAP's Interface:* FortiAP unit Ethernet and WiFi interfaces are bridged. • *Mesh Downlink*
Security Mode	The security mode for the SSID; one of: • *WPA-Personal*: The user must know the pre-shared key value to connect. • *WPA-Enterprise*: The user must know the user name and password to connect. • *Captive Portal*: The user connects to the open access point and then must authenticate to use the network. • *OPEN*
Data Encryption	The data encryption method for the SSID.
Maximum Clients	The maximum number of clients that can connect to the SSID at one time.
Last Modified	The date and time that the entry was last modified including the administrative user name of the user who made the change.

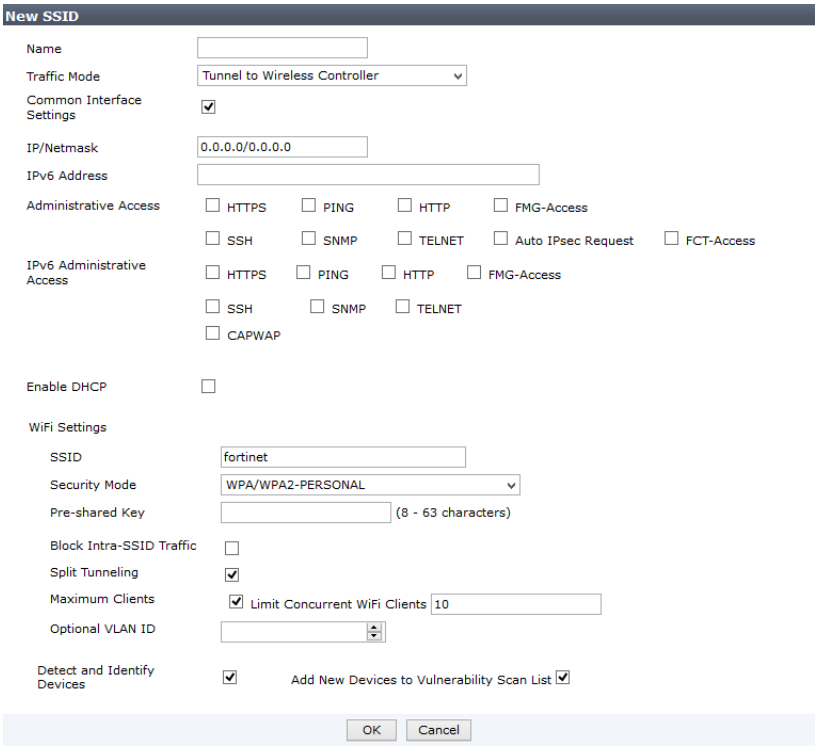
The following options are available:

Create New	Create a new SSID.
Delete	Select to delete the selected SSIDs.
Import	Select to import SSIDs.
Clone	Select an entry from this list, right-click and select *Clone* from the context menu to clone the entry.

Select All	Select an entry from this list, right-click and select *Select All* from the context menu. You can then right-click and select another action to perform on the selected entries.
Search	Search the SSIDs by typing a search term in the search field.
Column Settings	Right-click the column header to view and edit column settings. Column settings include the option to restore columns to their default state. Left-click column heading to drag-and-drop the column to change the column order.

To create a new SSID (Tunnel to wireless controller):

1. From the SSIDs page, select *Create New* in the toolbar. The *New SSID* window opens.



2. Enter the following information:

Name	Type a name for the SSID.
Traffic Mode	Select *Tunnel to Wireless Controller* from the drop-down list.
Common Interface Settings	Select to enable common interface settings.
IP/Netmask	Type the IP address and network mask.
IPv6 Address	Type the IPv6 address.

Administrative Access		Select the allowed administrative service protocols from: HTTPS, HTTP, PING, FMG-Access, SSH, SNMP, TELNET, Auto IPsec Request, and FCT-Access.
IPv6 Administrative Access		Select the allowed administrative service protocols from: HTTPS, HTTP, PING, FMG-Access, SSH, SNMP, TELNET, CAPWAP.
Enable DHCP		Select to enable and configure DHCP. This settings is only available when *Traffic Mode* is set to *Tunnel to Wireless Controller*.
	Address Range	Type the DHCP address range.
	Netmask	Type the netmask.
	Default Gateway	Select *Same As Interface IP* if the default gateway is the same as the interface IP, or select *Specify* and type a new gateway IP address.
	DNS Server	Select *Same As System DNS* if the DNS server is the same as the system DNS, or select *Specify* and type a DNS server address.
	MAC Address Access Control List	The MAC address control list allows you to view the MAC addresses and their actions. It includes a default entry for unknown MAC addresses. • Select *Create New* to create a new IP MAC binding. • Select an address and then select *Edit* to edit the default action for unknown MAC addresses or your IP MAC bindings. • Select an address or addresses and then select *Delete* to delete the selected items. The unknown MAC address cannot be deleted.
WiFi Settings		
	SSID	Type the wireless service set identifier (SSID) or network name for this wireless interface. Users who want to use the wireless network must configure their computers with this network name.
	Security Mode	Select a security mode. The options are: *WEP64*, *WEP128*, *WPA/WPA2-PERSONAL*, *WPA/WPA2-ENTERPRISE*, *Captive Portal*, *OPEN*, *WPA-ONLY-PERSONAL*, *WAP-ONLY-ENTERPRISE*, *WPA2-ONLY-PERSONAL*, or *WPA2-ONLY-ENTERPRISE*.
	Key Index	Select 1, 2, 3, or 4 from the drop-down menu. Many wireless clients can configure up to four WEP keys. Select which key clients must use.with this access point. This is available when `security` is a WEP type.
	Key	Type 10 Hex digits for the key value.
	Data Encryption	Select the data encryption method. The options are: *AES*, *TKIP*, and *TKIP-AES*. This option is only available when the security mode is set to WPA.

Pre-shared Key	Type the pre-shared key for the SSID. This option is only available when the security mode is set to *WPA-Personal*.
Detect and Identify Devices	Select to enable or disable detect and identify devices. When this setting is configured as enable, you can select to *Add New Devices to Vulnerability Scan List*.
Authentication	Select the authentication method for the SSID, either a RADIUS server or a user group, then select the requisite server or group from the respective drop-down list. This option is only available when the security mode is set to *WPA-Enterprise*.
Customize Portal Messages	Select to allow for customized portal messages. This option is only available when the security mode is set to *Captive Portal*.
User Groups	Select the user groups to add from the *Available* user group box. Use the arrow buttons to move the desired user groups to the *Selected* user groups box. This option is only available when the security mode is set to *Captive Portal*.
Block Intra-SSID Traffic	Select to block intra-SSID traffic.
Split Tunneling	Select to enable split tunneling.
Maximum Clients	Select to limit the concurrent WiFi clients that can connect to the SSID. If selected, type the desired maximum number of clients. Type 0 for no limit.
Optional VLAN ID	Select the VLAN ID in the text field using the arrow keys. Select 0 if VLANs are not used.
Detect and Identify Devices	Select to detect and identify devices connecting to the SSID.
Add New Devices to Vulnerability Scan List	Select to add new devices to the vulnerability scan list. This options is only available when *Detect and Identify Devices* is enabled.

3. Select *OK* to create the SSID.

To create a new SSID (Local bridge with FortiAP interface):

1. From the SSIDs page, select *Create New* in the toolbar. The *New SSID* window opens.
2. Enter the following information:

Name	Type a name for the SSID.
Traffic Mode	Select *Local bridge with FortiAP's Interface* from the drop-down list.

WiFi Settings		
	SSID	Type the wireless service set identifier (SSID) or network name for this wireless interface. Users who want to use the wireless network must configure their computers with this network name.
	Security Mode	Select a security mode. The options are: *WPA/WPA2-PERSONAL*, *WPA/WPA2-ENTERPRISE, OPEN*, *WPA-ONLY-PERSONAL*, *WAP-ONLY-ENTERPRISE*, *WPA2-ONLY-PERSONAL*, or *WPA2-ONLY-ENTERPRISE*.
	Pre-shared Key	Type the pre-shared key for the SSID. This option is only available when the security mode is set to *WPA-Personal*.
	Detect and Identify Devices	Select to enable or disable detect and identify devices. When this setting is configured as enable, you can select to *Add New Devices to Vulnerability Scan List*.
	Authentication	Select the authentication method for the SSID, either a RADIUS server or a user group, then select the requisite server or group from the respective drop-down list. This option is only available when the security mode is set to *WPA-Enterprise*.
	Split Tunneling	Select to enable split tunneling.
	Maximum Clients	Select to limit the concurrent WiFi clients that can connect to the SSID. If selected, type the desired maximum number of clients. Type 0 for no limit.
	Optional VLAN ID	Select the VLAN ID in the text field using the arrow keys. Select 0 if VLANs are not used.
Detect and Identify Devices		Select to detect and identify devices connecting to the SSID.
	Add New Devices to Vulnerability Scan List	Select to add new devices to the vulnerability scan list. This options is only available when *Detect and Identify Devices* is enabled.

3. Select *OK* to create the SSID.

To create a SSID (Mesh downlink):

1. From the SSIDs page, select *Create New* in the toolbar. The *New SSID* window opens.
2. Enter the following information:

Name	Type a name for the SSID.
Traffic Mode	Select *Mesh Downlink* from the drop-down list. T
WiFi Settings	

	SSID	Type the wireless service set identifier (SSID) or network name for this wireless interface. Users who want to use the wireless network must configure their computers with this network name.
	Security Mode	When *Traffic Mode* is set to *Mesh Downlink*, the security mode options are: *WPA/WPA2-PERSONAL*, *OPEN*, *WPA-ONLY-PERSONAL*, or *WPA2-ONLY-PERSONAL*.
	Pre-shared Key	Type the pre-shared key for the SSID. This option is only available when the security mode is set to *WPA-Personal*.
	Detect and Identify Devices	Select to enable or disable detect and identify devices. When this setting is configured as enable, you can select to *Add New Devices to Vulnerability Scan List*.
	Split Tunneling	Select to enable split tunneling.
	Optional VLAN ID	Select the VLAN ID in the text field using the arrow keys. Select 0 if VLANs are not used.
Detect and Identify Devices		Select to detect and identify devices connecting to the SSID.
	Add New Devices to Vulnerability Scan List	Select to add new devices to the vulnerability scan list. This options is only available when *Detect and Identify Devices* is enabled.

3. Select *OK* to create the SSID.

To edit an SSID:

1. From the SSIDs page, double click on an SSID name or right-click on the name and select *Edit* from the pop-up menu. The *Edit SSID* window opens.
2. Edit the settings as required. The SSID name cannot be edited.
3. Selected *OK* to apply your changes.

To delete an SSID or SSIDs:

1. Select the SSID or SSIDs that you would like to delete from the SSID list.
2. Select *Delete* or right click on the SSID and select *Delete* from the pop-up menu.
3. Select *OK* in the confirmation dialog box to delete the SSID or SSIDs.

To clone an SSID:

1. From the SSIDs page, right-click on the SSID name and select *Clone* from the pop-up menu.The *Clone SSID* window opens.
2. Edit the settings as required.
3. Selected *OK* to clone the SSID.

To import an SSID:

1. From the SSIDs page, select *Import* in the toolbar. The *Import SSID* dialog box opens.
2. Enter the following information:

Import from device	Select a device from which to import the SSID or SSIDs from the drop-down list. This list will include all the devices available in the ADOM.
Virtual Domain	Is applicable, select the virtual domain from which the SSIDs will be imported.
Available Objects List	The available objects that can be imported. Select an object or objects and then select the down arrow to move the selected object or objects to the *Selected Objects List*.
Selected Objects List	The objects that are to be imported. To remove an object or objects from the list, select the object or objects and then select the up arrow. The selected items will be moved back to the *Available Objects List*.
New Name	Select to create a new name for the object or objects that are being imported, and then type the name in the field.

3. Select *OK* to import the SSID or SSIDs.

Custom AP profiles

The custom AP profiles menu lists all of the custom AP profiles available in the ADOM. Profiles can be created, edited, cloned, deleted, imported, and searched.

To view the custom AP profiles, in the *Provisioning Templates* tree menu, select an ADOM, then select *WiFi Templates* > *Custom AP Profiles*.

The following information is available:

Name	The profile's name.
Comments	Comments about the profile.
Platform	The platform that the custom AP profile applies to.
Radio 1	The function of the Radio 1 in the profile.
Radio 2	If applicable, the Radio 2 function in the profile.
Last Modified	The date and time that the entry was last modified including the administrative user name of the user who made the change.

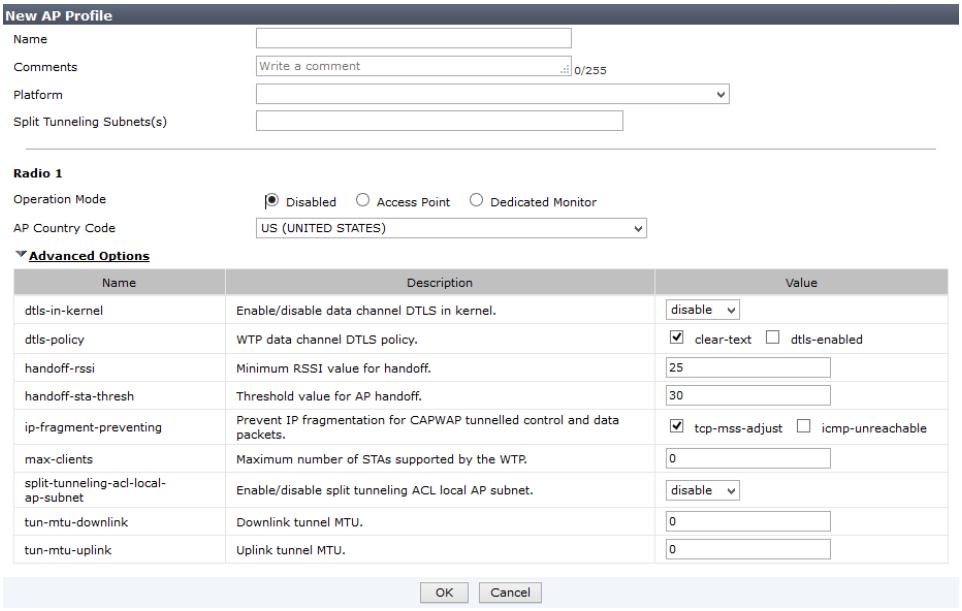
The following options are available:

Create New	Create a new custom AP profile.

Delete	Select to delete the selected custom AP profiles.
Import	Select to import custom AP profiles.
Clone	Select an entry from this list, right-click and select *Clone* from the context menu to clone the entry.
Select All	Select an entry from this list, right-click and select *Select All* from the context menu. You can then right-click and select another action to perform on the selected entries.
Search	Search the custom AP profiles by entering a search term in the search field.
Column Settings	Right-click the column header to view and edit column settings. Column settings include the option to restore columns to their default state. Left-click column heading to drag-and-drop the column to change the column order.

To create a new custom AP profile (Radio operation mode disabled):

1. From the custom AP profiles page, select *Create New*. The *New AP Profile* window opens.



2. Enter the following information:

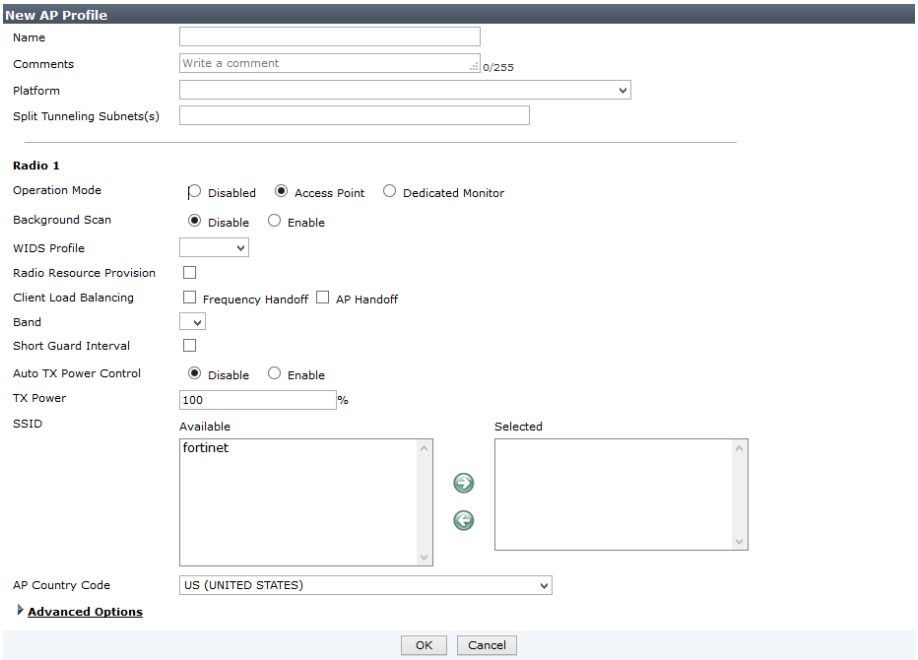
Name	Type a name for the profile.
Comment	Optionally, type comments.
Platform	Select the platform that the profile will apply to from the drop-down list.
Split Tunneling Subnet(s)	Type the split tunneling subnet(s).

Radio 1 & 2	Configure the radio settings. The Radio 2 settings will only appear if applicable to the platform that is selected.
Operation Mode	Select *Disabled*.
AP Country Code	Select the access point country code from the drop-down list.
Advanced Options	Configure advanced options for the SSID. • *dtsl-in-kernal*: Select to enable or disable data channel DTLS in kernel. • *dtls-policy*: Select clear-text, dtls-enable, or both. • *handoff-rssi*: Type a value for RSSI handoff. • *handoff-sta-thresh*: Type a value for the threshold. • *ip-fragment-preventing*: Prevent IP fragmentation for CAPWAP tunnelled control and data packets. Select *tcp-mss-adjust*, *icmp-unreachable*, or both. • *max-clients*: Type a value for the maximum number of clients. • *split-tunneling-acl-local-ap-subnet*: Select to enable or disable split tunneling ACL local AP subnet. • *tun-mtu-downlink*: Type the downlink tunnel MTU. • *tun-mtu-uplink*: Type the uplink tunnel MTU.

3. Select *OK* to create the new wireless profile.

To create a new custom AP profile (Radio operation mode Access Point):

1. From the custom AP profiles page, select *Create New*. The *New AP Profile* window opens.



2. Enter the following information:

Name	Type a name for the profile.
Comment	Optionally, type comments.
Platform	Select the platform that the profile will apply to from the drop-down list.
Split Tunneling Subnet(s)	Type the split tunneling subnet(s).
Radio 1 & 2	Configure the radio settings. The Radio 2 settings will only appear if applicable to the platform that is selected.
Operation Mode	Select *Access Point* (default).
Background Scan	Enable or disable background scanning.
WIDS Profile	Select a WIDS profile from the drop-down list.
Rogue AP On-Wire Scan	Select to enable rogue AP on-wire scan. This option is only available is the operation mode is set to *Dedicated Monitor*, or if background scan is enabled.
Radio Resource Provision	Select to enable radio resource provisioning.
Client Load Balance	Select the client load balancing methods to use. Frequency and/or AP handoff can be used.
Band	Selected the wireless band from the drop-down list. The bands available are dependent on the platform selected.
Channel	Select the channel or channels that are available. The channels available are dependent on the platform selected.
Auto TX Power Control	Enable or disable automatic TX power control.
TX Power	If *Auto TX Power Control* is disabled, type the TX power in the form of the percentage of the total available power.
TX Power Low	If *Auto TX Power Control* is enabled, type the minimum TX power in dBm.
TX Power High	If *Auto TX Power Control* is enabled, type the maximum TX power in dBm.
SSID	Select available SSIDs from the *Available* box, and move them to the *Selected* box using the arrow buttons to select the SSIDs to apply to this profile.
AP Country Code	Select the access point country code from the drop-down list.
Advanced Options	For more information, see Advanced Options on page 185.

3. Select *OK* to create the new wireless profile.

To create a new custom AP profile (Radio operation mode Dedicated Monitor):

1. From the custom AP profiles page, select *Create New*. The *New AP Profile* window opens.
2. Enter the following information:

Name	Type a name for the profile.
Comment	Optionally, type comments.
Platform	Select the platform that the profile will apply to from the drop-down list.
Split Tunneling Subnet(s)	Type the split tunneling subnet(s).
Radio 1 & 2	Configure the radio settings. The Radio 2 settings will only appear if applicable to the platform that is selected.
WIDS Profile	Select a WIDS profile from the drop-down list.
Rogue AP On-Wire Scan	Select to enable rogue AP on-wire scan.
AP Country Code	Select the access point country code from the drop-down list.
Advanced Options	For more information, see Advanced Options.

3. Select *OK* to create the new wireless profile.

To edit a custom AP profile:

1. From the custom AP profiles page, double click on a wireless profile's name or right-click on the name and select *Edit* from the pop-up menu. The *Edit AP Profile* window opens.
2. Edit the settings as required. The profile name cannot be edited.
3. Select *OK* to apply your changes.

To delete a custom AP profile:

1. Select the custom AP profile that you would like to delete from the profile list.
2. Select *Delete* or right click on the profile and select *Delete* from the pop-up menu.
3. Select *OK* in the confirmation dialog box to delete the profile.

To clone a custom AP profile:

1. From the custom AP profiles page, right-click on a profile name and select *Clone* from the pop-up menu. The *Edit AP Profile* window opens.
2. Edit the name of the profile, then edit the remaining settings as required.
3. Select *OK* to clone the profile.

To import a AP profile:

1. From the AP profile page, select *Import* in the toolbar. The *Import AP Profile* dialog box opens.
2. Enter the following information:

Import from device	Select a device from which to import the profile or profiles from the drop-down list. This list will include all the devices available in the ADOM.
Virtual Domain	Is applicable, select the virtual domain from which the profile will be imported.
Available Objects List	The available objects that can be imported. Select an object or objects and then select the down arrow to move the selected object or objects to the *Selected Objects List*.
Selected Objects List	The objects that are to be imported. To remove an object or objects from the list, select the object or objects and then select the up arrow. The selected items will be moved back to the *Available Objects List*.
New Name	Select to create a new name for the item or items that are being imported, and then type the name in the field.

3. Select *OK* to import the profile or profiles.

WIDS Profile

The WIDS monitors wireless traffic for a wide range of security threats by detecting and reporting on possible intrusion attempts. When an attack is detected, a log message is recorded.

WIDS profiles can be created, edited, cloned, deleted, imported, and searched. A default profile is available by default.

To view the wireless profiles, in the *Provisioning Templates* tree menu, select an ADOM, then select *WiFi Templates* > *WIDS Profiles*. The WIDS profile list is displayed, with the following information is available:

Name	The profile's name.
Comments	Comments about the profile.
Last Modified	The date and time that the entry was last modified including the administrative user name of the user who made the change.

The following options are available:

Create New	Create a new WIDS profile.
Delete	Select to delete the selected WIDS profiles.
Import	Select to import WIDS profiles.

Clone	Select an entry from this list, right-click and select *Clone* from the context menu to clone the entry.
Search	Search the WIDS profiles by entering a search term in the search field.
Column Settings	Right-click the column header to view and edit column settings. Column settings include the option to restore columns to their default state. Left-click column heading to drag-and-drop the column to change the column order.

To create a new WIDS profile:

1. From the WIDS profiles page, select *Create New*. The *New Wireless Intrusion Detection System Profile* window opens.
2. Enter the following information:

Name	Type a name for the profile.
Comments	Optionally, type comments.
Enable Rogue AP Detection	Select to enable rogue AP detection.
Background Scan Every Second(s)	Type a value in the text field.
Disable Background Scan During Specified Time	When selected, select the day of week, start, and stop time.
Enable Passive Scan Mode	Select to enable passive scan mode.
Enable On-Wire Rogue AP Detection	Select to enable on-wire rogue AP detection. When enabled you can select to auto suppress rogue APs in foreground scan.
Intrusion Type	The intrusion types that can be detected.
Status	Select the status of the intrusion type (enable it).
Threshold	If applicable, type a threshold for reporting the intrusion, in seconds except where specified.
Interval (sec)	If applicable, type the interval for reporting the intrusion, in seconds.

3. Select *OK* to create the new WIDS profile.

The following table provides a list of intrusion types and their descriptions.

Intrusion Type	Description
Asleap Attack	ASLEAP is a tool used to perform attacks against LEAP authentication.
Association Frame Flooding	A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
Authentication Frame Flooding	A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
Broadcasting De-authentication	This is a type of Denial of Service attack. A flood of spoofed de-authentication frames forces wireless clients to de-authenticate, then re-authenticate with their AP.
EAPOL Packet Flooding (to AP)	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the AP with these packets can be a denial of service attack. Several types of EAPOL packets can be detected: EAPOL-FAIL, EAPOL-LOGOFF, EAPOL-START, and EAPOL-SUCC.
Invalid MAC OU	Some attackers use randomly-generated MAC addresses. The first three bytes of the MAC address are the Organizationally Unique Identifier (OUI), administered by IEEE. Invalid OUIs are logged.
Long Duration Attack	To share radio bandwidth, WiFi devices reserve channels for brief periods of time. Excessively long reservation periods can be used as a denial of service attack. You can set a threshold between 1000 and 32 767 microseconds. The default is 8200.
Null SSID Probe Response	When a wireless client sends out a probe request, the attacker sends a response with a null SSID. This causes many wireless cards and devices to stop responding.
Premature EAPOL Packet Flooding (to client)	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the client with these packets can be a denial of service attack. Two types of EAPOL packets can be detected: EAPOL-FAIL, and EAPOL-SUCC.
Spoofed De-authentication	Spoofed de-authentication frames form the basis for most denial of service attacks.
Weak WEP IV Detection	A primary means of cracking WEP keys is by capturing 802.11 frames over an extended period of time and searching for patterns of WEP initialization vectors (IVs) that are known to be weak. WIDS detects known weak WEP IVs in on-air traffic.
Wireless Bridge	WiFi frames with both the FromDS and ToDS fields set indicate a wireless bridge. This will also detect a wireless bridge that you intentionally configured in your network.

To edit a WIDS profile:

1. From the WIDS profiles page, double click on a profile's name or right-click on the name and select *Edit* from the pop-up menu. The *Edit Wireless Intrusion Detection System Profile* window opens.
2. Edit the settings as required.
3. Selected *OK* to apply your changes.

To delete a WIDS profile:

1. Select the WIDS profile that you would like to delete from the profile list.
2. Select *Delete* or right click on the profile and select *Delete* from the pop-up menu.
3. Select *OK* in the confirmation dialog box to delete the profile.

To clone a WIDS profile:

1. From the WIDS profiles page, right-click on a profile name and select *Clone* from the pop-up menu. The *Edit Wireless Intrusion Detection System Profile* window opens.
2. Edit the name of the profile, then edit the remaining settings as required.
3. Select *OK* to clone the profile.

To import a WIDS profile:

1. From the WIDS profile page, select *Import* in the toolbar. The *Import WIDS Profile* dialog box opens.
2. Enter the following information:

Import from device	Select a device from which to import the profile or profiles from the drop-down list. This list will include all the devices available in the ADOM.
Virtual Domain	Is applicable, select the virtual domain from which the profile will be imported.
Available Objects List	The available objects that can be imported. Select an object or objects and then select the down arrow to move the selected object or objects to the *Selected Objects List*.
Selected Objects List	The objects that are to be imported. To remove an object or objects from the list, select the object or objects and then select the up arrow. The selected items will be moved back to the *Available Objects List*.
New Name	Select to create a new name for the item or items that are being imported, and then type the name in the field.

3. Select *OK* to import the profile or profiles.

Threat Weight templates

User or client behavior can sometimes increase the risk of being attacked or becoming infected. For example, if one of your network clients receives email viruses on a daily basis while no other clients receive these

attachments, extra measures may be required to protect that client, or a discussion with the user about this issue may be warranted.

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

Threat weight profiles can be created, edited, and assigned to devices. When creating a profile, the default threat level definitions are used; these can be changed later. When Threat Weight Tracking is enabled, the *Log Allowed Traffic* setting will be enabled on all policies. For more information on configuring the Threat Weight profile, see the *FortiOS 5.2 Handbook*.

In FortiOS v5.2, *Client Reputation* has been renamed *Threat Weight Tracking*. In FortiOS, this feature is found at *Security Profiles* > *Advanced* > *Threat Weight*.

To create a new threat weight profile:

1. Go to the *Threat Weight Templates* > *Threat Weight* page and select *Create New* in the toolbar.
2. In the *New Threat Weight Profile* window, type a name for the profile.
3. Select *OK* to create the new threat weight profile.

To edit a threat weight profile:

1. Right-click in the profile row and select *Edit* from theright-click menu. The *Threat Level Definition* page opens.
2. Adjust the threat levels as needed:

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

3. Select *OK* to save your changes and close the page.

To assign a threat weight profile to a device:

1. Right-click in the profile row and select *Assigned Devices* from the right-click menu.
2. Add or remove devices as needed in the *Assigned Devices* dialog box, then select *OK*. Select the add icon to add multiple devices.

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

FortiClient templates

The FortiClient templates menu allows you to create and manage FortiClient profiles which can then be assigned to devices.

FortiClient templates are available in v5.0 and v5.2 ADOMs only. Some settings may not be available in all ADOM versions.

Endpoint control ensures that workstation computers (endpoints) and other network devices meet security requirements, otherwise they are not permitted access. Endpoint Control enforces the use of FortiClient Endpoint Security and pushes a FortiClient Profile to the FortiClient application.

The following information is displayed:

Name	The name of the FortiClient profile. Right-click the column heading to change the FortiClient profile order.
User	The device groups, user groups, and users associated with the FortiClient profile.
Comments	Optional FortiClient profile comments.
Last Modified	The date and time that the entry was last modified including the administrative user name of the user who made the change.

The following options are available:

Create New	Select to create a new FortiClient profile.
Delete	Select an entry from the list and select *Delete* from the toolbar. Optionally, select an entry from the list, right-click and select *Delete* from the context menu to delete the entry.
Import	Select to import a FortiClient profile from an existing device in the ADOM.
Edit	Select an entry from the list, right-click and select *Edit* from the context menu to edit the entry. Alternatively, double click the entry to open the *Edit FortiClient Profile* page.

Clone	Select an entry from the list, right-click and select *Clone* from the context menu to clone the entry.
Search	Search the FortiClient profiles by entering a search term in the search field.
Column Settings	Right-click the column header to view and edit column settings. Column settings include the option to restore columns to their default state. Left-click column heading to drag-and-drop the column to change the column order.

FortiClient Profiles

The FortiClient profile consists of the following sections:

- Antivirus Protection
- Web Category Filtering
  - Client Web Filtering when On-Net
- VPN
  - Client VPN Provisioning
  - Auto-connect When Off-Net
- Application Firewall
- Use FortiManager for client software/signature update
  - Failover to FDN when FortiManager is not available
- Dashboard Banner
- Client-based Logging When On-Net
- iOS settings
- Android settings

Non-compliant endpoints are those without the latest version of FortiClient installed. They can be sent to the FortiClient download portal to obtain FortiClient software, or they can be blocked. For more information on configuring FortiClient Profiles and Endpoint Control, see the *FortiClient Administration Guide*.

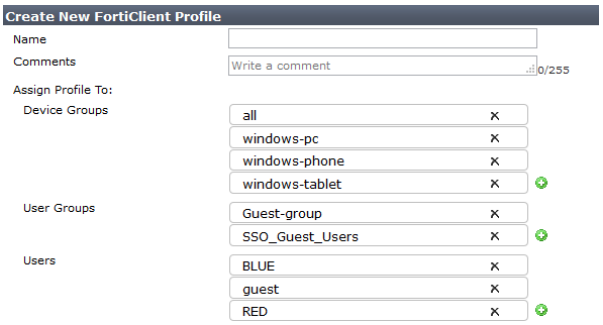
When a FortiClient Profile is selected in a firewall policy, all users of that firewall policy must have FortiClient Endpoint Security installed. The FortiClient profile settings are pushed to the FortiClient application on the client.

FortiClient profiles can be created, edited, cloned, deleted, and imported from devices using right-click menu and toolbar selections.

In FortiOS v5.2, *Endpoint Profile* has been renamed *FortiClient Profiles*. In FortiOS, this feature is found at *User & Device* > *FortiClient Profiles*.

To create a new FortiClient profile:

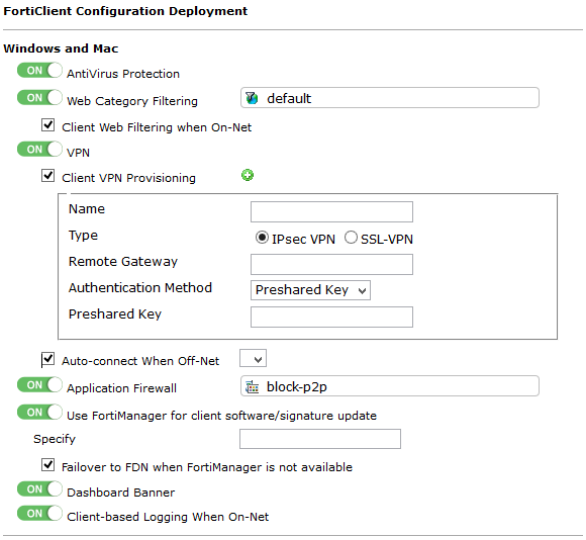
1. Go to the *FortiClient Templates* > *FortiClient Profile* page and select *Create New*. The *Create New FortiClient Profile* page opens.



2. Enter the following information:

Name	Type a name for the new FortiClient profile. When creating a new FortiClient profile, XSS vulnerability characters are not allowed.
Comments	Type a profile description. (optional)
Assign to Profile To:	• Device Groups: Select device groups in the drop-down menu. Select the add icon to assign multiple device groups to the FortiClient profile, for example Mac and Windows PC. • User Groups: Select user groups in the drop-down menu. Select the add icon to assign multiple user groups to the FortiClient profile. • Users: Select users in the drop-down menu. Select the add icon to assign multiple users to the FortiClient profile. You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN.

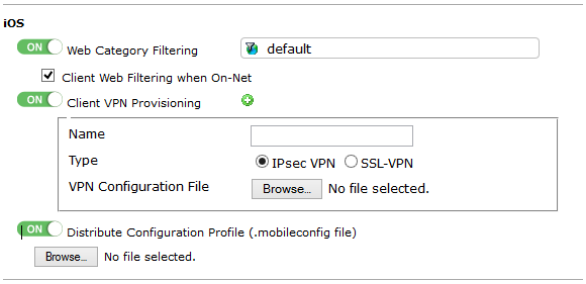
3. Continue down the page to the operating system specific settings.



4. Enter the following information for the Windows and Mac section:

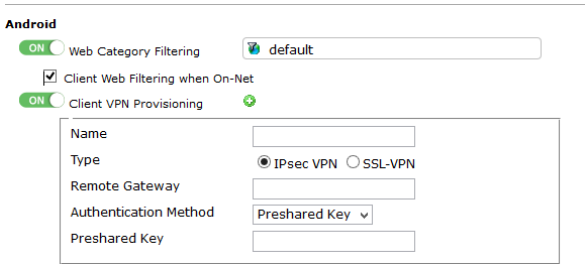
Antivirus Protection	Toggle the button to enable or disable this feature.
Web Category Filtering	Toggle the button to enable or disable this feature. When enabled, you can select a web filter profile in the drop-down list.
Client Web Filtering when On-Net	Select the checkbox to enable client web filtering when on-net. FortiClient determines the client to be on-net when the registered FortiGate serial number matches one of the serial numbers it gets from the FortiGate DHCP server. Otherwise it is off-net.
VPN	Toggle the button to enable or disable this feature.
Client VPN Provisioning	When enabled, you can configure multiple IPsec VPN and SSL VPN connections. Select the add icon to add multiple VPN connections. Select the delete icon to remove VPN connections. Type the VPN name, type, remote gateway, and authentication method information.
Auto-connect When Off-Net	You can select to auto-connect to a specific VPN when the client is off. Select the name of the VPN connection the drop-down list.
Application Firewall	Toggle the button to enable or disable this feature. When enabled, you can select an application control sensor in the drop-down list.
Use FortiManager for client software/signature update	Toggle the button to enable or disable this feature. When enabled, you can specify the IP address of the FortiManager.
Failover to FDN when FortiManager not available	Select the checkbox to failover to the FortiGuard Distribution Network when the FortiManager is not available.
Dashboard Banner	Toggle the button to enable or disable this feature. When enabled FortiClient advertisements will be displayed.
Client-based Logging When On-Net	Toggle the button to enable or disable this feature. FortiClient determines the client to be on-net when the registered FortiGate serial number matches one of the serial numbers it gets from the FortiGate DHCP server. Otherwise it is off-net.

5. If required, configure the *FortiClient Configuration Deployment* settings for *iOS*:



Web Category Filtering	Click the ON/OFF button to enable or disable this feature. When enabled, you can select a web filter profile in the drop-down menu. Select the checkbox to enable client web filtering when on-net. FortiClient determines the client to be on-net when the registered FortiGate serial number matches one of the serial numbers it gets from the FortiGate DHCP server. Otherwise it is off-net.
Client VPN Provisioning	Enable to configure the FortiClient VPN client. Select the add icon to add multiple VPN connections. Select the delete icon to remove VPN connections. Optionally, you can upload the FortiClient iOS VPN configuration file.
Name	Type a name to identify this VPN configuration in the FortiClient application.
Type	Select *IPsec VPN* or *SSL VPN*. • If you select *IPsec VPN*, select a *VPN Configuration File* that contains the required IPsec VPN configuration. The Apple iPhone Configuration Utility/Apple Configurator produces `.mobileconfig` files which contain configuration information for an iOS device. • If you select *SSL VPN*, type the VPN configuration details.
Distribute Configuration Profile	Distribute configuration information to iOS devices running FortiClient Endpoint Security. Select *Browse* and locate the file to be distributed. The Apple iPhone Configuration Utility/Apple Configurator produces `.mobileconfig` files which contain configuration information for an iOS device.

6. If required, configure the *FortiClient Configuration Deployment* settings for *Android*:



Web Category Filtering	Click the ON/OFF button to enable or disable this feature. When enabled, you can select a web filter profile in the drop-down menu. Select the checkbox to enable client web filtering when on-net. FortiClient (Android) only supports FortiGuard Categories settings in the Web Filter Profile. Only Allow and Block actions are supported. All other settings will be ignored by FortiClient (Android).
Client VPN Provisioning	Enable to configure the FortiClient VPN client. Select the add icon to add multiple VPN connections. Select the delete icon to remove VPN connections.

Name	Type a name to identify this VPN configuration in the FortiClient application.
Type	Select *IPsec VPN* or *SSL VPN*.
Remote Gateway	Type the remote gateway.
Authentication Method	Select the authentication method to use, either *Preshared Key* or *Certificate*. If *Preshared Key* is selected, type the your pre-shared key. This option is only available if the type is *IPsec VPN*.
Require Certificate	Select to require a certificate. This option is only available if the type is *SSL-VPN*.
Access Port	Type the access port number. This option is only available if the type is *SSL-VPN*.

7. Select *OK*.

To edit a FortiClient profile:

1. Double-click on the profile name, or right-click in the profile row and select *Edit* from the pop-up menu.
2. Edit the settings as required in the *Edit FortiClient Profile* window, then select *OK* to apply the changes.

To delete a FortiClient profile:

1. Right-click in the profile row and select *Delete* from the pop-up menu.
2. Select *OK* in the confirmation dialog box to delete the profile.

To clone a FortiClient profile:

1. Right-click in the row of the profile that you are cloning and select *Clone* from the pop-up menu.
2. In the *Edit FortiClient Profile* window, change the name of the FortiClient profile.
3. Adjust the remaining settings as required, then select *OK* to create the cloned profile.

To import a FortiClient profile:

1. From the FortiClient profile page, select *Import* in the toolbar.
2. Enter the following information in the *Import FortiClient Profile* dialog box:

Import from device	Select a device from which to import the profile or profiles from the drop-down list. This list will include all the devices available in the ADOM.
Virtual Domain	Is applicable, select the virtual domain from which the profile will be imported.
Available Objects List	The available objects that can be imported. Select an object or objects and then select the down arrow to move the selected object or objects to the *Selected Objects List*.

Selected Objects List	The objects that are to be imported. To remove an object or objects from the list, select the object or objects and then select the up arrow. The selected items will be moved back to the *Available Objects List*.
New Name	Select to create a new name for the item or items that are being imported, and then type the name in the field.

3. Select *OK* to import the profile.

Certificate templates

The certificate templates menu allows you to create CA certificate templates, add devices to them, and then generate certificates for selected devices. Once the CA certificates have been generated and signed, they can be installed using the install wizard.

Certificate templates are available in v4.3, v5.0, and v5.2 ADOMs. Some settings may not be available in all ADOM versions.

The following information is displayed:

Device Name	The device name is displayed.
Certificate Status	The certificate status is displayed.

The following options are available:

Add Device	Select to add a device. Select *OK* to save the setting.
Delete Device	Select an entry, right-click, and select Delete Device from the menu. A confirmation dialog box is displayed. Select OK to proceed with the delete action.
Generate	Select to generate the certificate request.
Create New	Select to create a new certificate.
Edit	Select a certificate template, right-click and select *Edit* to edit the selected certificate.
Delete	Select a certificate template, right-click and select *Delete* to delete the selected certificate. Select *OK* in the confirmation dialog box to complete the delete action.

To create a new certificate template:

1. In the *Provisioning Templates* tree menu, right-click on *Certificate Templates* and select *Create New* from the pop-up menu. The *New Certificate* dialog box opens.
2. Enter the following information:

Certificate Name	Type a name for the certificate.
Optional Information	Optionally, type the organization unit, organization, locality (city), province or state, country or region, and email address.
Key Type	RSA is the default key type. This field cannot be edited.
Key Size	Select the key size from the drop-down list. The available key sizes are: • 512 Bit • 1024 Bit • 1536 Bit • 2048 Bit
Online SCEP Enrollment	
CA Server URL	Type the CA server URL.
Challenge Password	Type the challenge password for the CA server.

3. Select *OK* to create the certificate.

To edit a certificate:

1. Right-click on the certificate name in the tree menu and select *Edit* from the pop-up menu.
2. Edit the settings as required in the *Edit Certificate* window, then select *OK* to apply the changes.

To delete a certificate:

1. Right-click on the certificate name in the tree menu and select *Delete* from the pop-up menu.
2. Select *OK* in the confirmation dialog box to delete the certificate.

To add device to a certificate template:

1. Select the certificate template from the tree menu to which you are adding devices.
2. In the content pane, select *Add Device* from the toolbar. The *Add Device* dialog box opens.
3. Add devices from the drop-down list, then select *OK* to add the devices.

To generate certificates:

1. Do one of the following:
   - Select one or more devices from the list of devices added to the certificate template, and then select *Generate* from the toolbar.
   - Right-click on a device from the list and select *Generate* from the pop-up menu.
2. Confirm the certificate generation in the confirmation dialog box to generate the certificate.

If a certificate failed generation, you can attempt to generate the certificate again.

If the certificate name already exists on the FortiGate unit, it will be overwritten each time the generate button is run. This allows the certificates to be updated more easily (for instances, if it has expired or is about to expire) without affecting any existing VPN configurations that are using the certificate.

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 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 serial number, firmware version, and other explicitly entered information. You can also select to assign a system template to the provisioned device.
- 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. You can select to create a revision and schedule the install.
  - *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. This option is only available when launching the *Install Wizard* in the Device Manager tab.
- Import policy wizard
  - *Import device*
- Re-install policy
  - *Re-install Policy Package*: You can right-click on the *Config Status* column icon in the Device Manager tab 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 GUI page to access these options.

Add device wizard

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

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

To launch the Add Device wizard, click the *Add Device* icon in the toolbar. Alternatively, you can right-click an item in the tree menu and select *Add Device* in the menu.

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

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

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

Add a device using discover mode

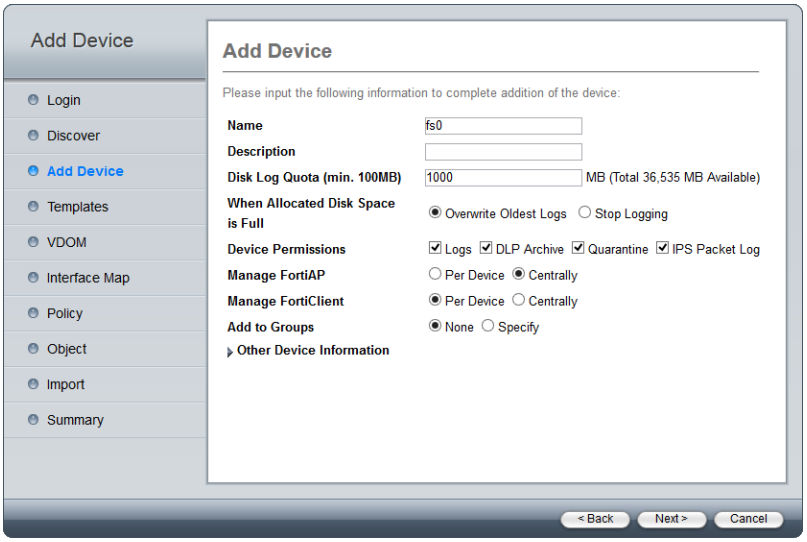
The following steps will guide you through the *Add Device* wizard phases to add a device using *Discover* mode.

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

1. Launch the *Add Device* wizard.
2. Select *Discover*, and enable *Import Device* on the *Login* phase page.
3. Type the IP address, user name, and password for the device, then select *Next*.
   The FortiManager will probe the IP address on your network to discover device details, including:
   - IP address
   - Administrator user name
   - Device model
   - Firmware version (build)
   - Serial number
   - High Availability mode

Only stop on Add/Import Error	Enable this optionto only stop the wizard when encountering add or import errors. This option is not available when importing devices with VDOMs enabled.
Import Device Policy & Objects	Select this option to import policies and objects from the device that is being added.

4. Select *Next* to continue to the *Add Device* page.



5. Configure the following settings:

Name	Type a unique name for the device. The device name cannot contain spaces or special characters.
Description	Type a description of the device (optional).
Disk Log Quota (min. 100MB)	Type a value for the disk log quota in MB. The minimum value is 100MB. The total available space in MB is listed to the right of the text field.
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*
Manage FortiAP	Enable or disable central FortiAP management.
Manage Endpoint	Enable or disable central endpoint control. Select *Specify* and select the groups that you want the device to belong to.
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*

6. Select *Next*.

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

   - Discovering device
   - Promoting unregistered device
   - Checking device status
   - Creating device database
   - Updating high availability status
   - Retrieving interface information
   - Retrieving configuration
   - Loading to database
   - Creating initial configuration file
   - Retrieving IPS signature information
   - Retrieving support data
   - Updating group membership

7. Select *Next* to continue.

8. System templates can be used to centrally manage certain device-level options from a central location.

   If required, assign a system template using the drop-down menu. Alternatively, you can select to configure all settings per-device inside *Device Manager*. For more information, see Provisioning Templates on page 173.

9. Select *Next* to continue.

   If VDOMs are not enabled on the device, the wizard will skip the VDOM phase. You can Select to import each VDOM step by step, one at a time, or automatically import all VDOMs.

   The following import options are available:

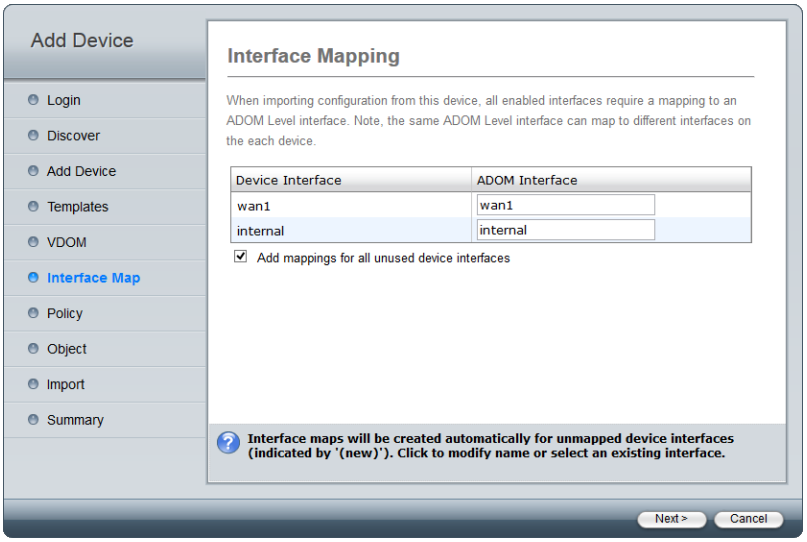
Import Options	The wizard will detect if the device contains virtual domains (VDOMs). You can select the behavior for FortiManager to take to import these VDOMs. Import options include: • *Import each VDOM step by step* • *Import VDOM one at a time* • *Automatically import all VDOMs*

10. Select *Next* to complete the VDOM import.

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

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

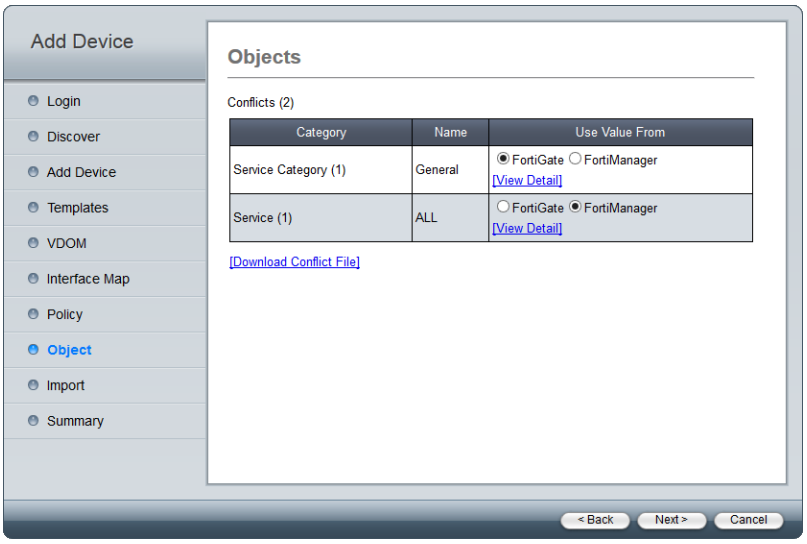
When importing configurations from a device, all enabled interfaces require a mapping.



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

    Choose a folder from the drop-down list, type a new policy package name, and select the policies and objects that need to be imported.

15. Select *Next* to continue. The wizard searches the unit for objects to import, and reports any conflicts it detects. If conflicts are detected, you must decide whether to use the FortiGate value or the FortiManager value.



If there are conflicts, you can select *View Details* to view details of each individual conflict, or you can download an HTML conflict file to view all the details about the conflicts.

16. Select *Next*. The objects that are ready to be imported are shown.
17. Select *Next* to import policies and objects into the database.
18. Select *Next*.

    A detailed summary of the import is shown, and the Import Report can be downloaded. This report is only available on this page.

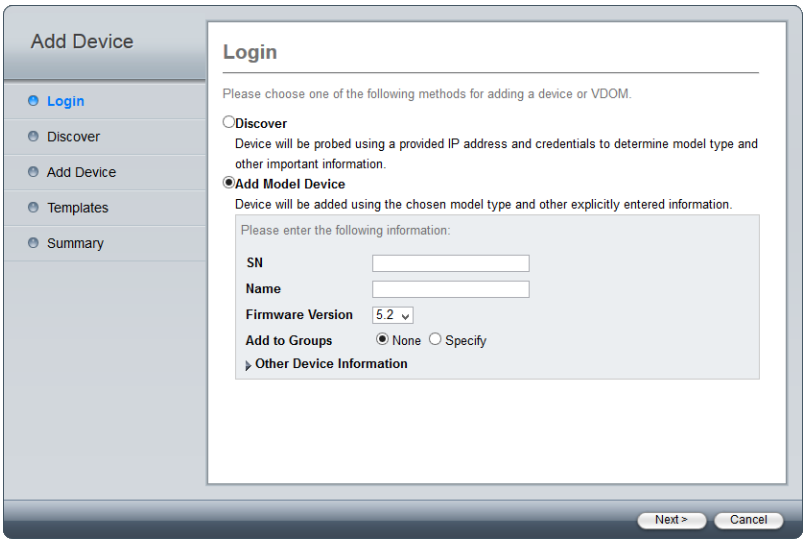
19. Select *Finish* to close the wizard.

Add a model device

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

When adding devices to product specific ADOMs, you can only add this model type to the ADOM. When selecting to add a non-FortiGate device to the root ADOM, the device will automatically be added to the product specific ADOM.

1. Launch the *Add Device* wizard.
2. Select *Add Model Device* on the *Login* page.



Enter the following information:

Add Model Device	Device will be added using the chosen model type and other explicitly entered information.
SN	Type the device serial number. This field is mandatory.
Name	Type a descriptive name for the device. This name is displayed in the *Device Name* column.
Firmware Version	Select the device firmware version from the drop-down list.
Add to Groups	Select to add the device to existing device groups.
Other Device Information	Optionally, you can type other device information including company/organization, contact, city, province/state, and country.

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

Each device must have a unique name, otherwise the wizard will fail.

4. Select *Next*. The *Templates* page is displayed.
5. System templates can be used to centrally manage certain device-level options from a central location.

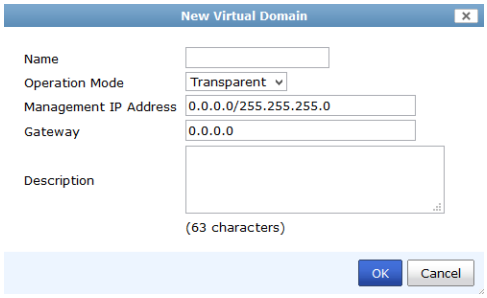
   If required, assign a system template using the drop-down menu. Alternatively, you can select to configure all settings per-device inside *Device Manager*. For more information, see Provisioning Templates on page 173.
6. Select *Next* to proceed to the summary page.
7. Select *Finish* to exit the wizard.

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

Add a VDOM to a device

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

The number of VDOMs you can add is dependent on the device model. For more information, see the *Maximum Values Table* in the Fortinet Document Library.



The following settings are available:

Name	Type a name for the new virtual domain.
Operation Mode	Select either *NAT* or *Transparent*.
Management IP Address	Type the management IP address and network mask for the VDOM. This setting is available when *Operation Mode* is *Transparent*.
Gateway	Type the gateway IP address. This setting is available when *Operation Mode* is *Transparent*.
Description	Optionally, enter a description of the VDOM.

Install wizard

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

Launching the install wizard

To launch the *Install* wizard, select the *Install* icon in the toolbar. To launch the *Install* wizard from the *Policy & Objects* tab, right-click on the policy package and select *Install Wizard.*

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

- Install policy package and device settings: Install a selected policy package. Any device specific settings for devices associated with package will also be included.
- Installing 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. This option is only available when launching the *Install Wizard* in the Device Manager tab.

- Installing interface policy (only): Install interface policy only in a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Install policy package and device settings

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

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

3. Select *Next* to continue.

Device selection

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

Validation

The *Validation* page checks the following:

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

Devices with a validation error will be skipped for installation.

The following options are available:

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

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

Installation

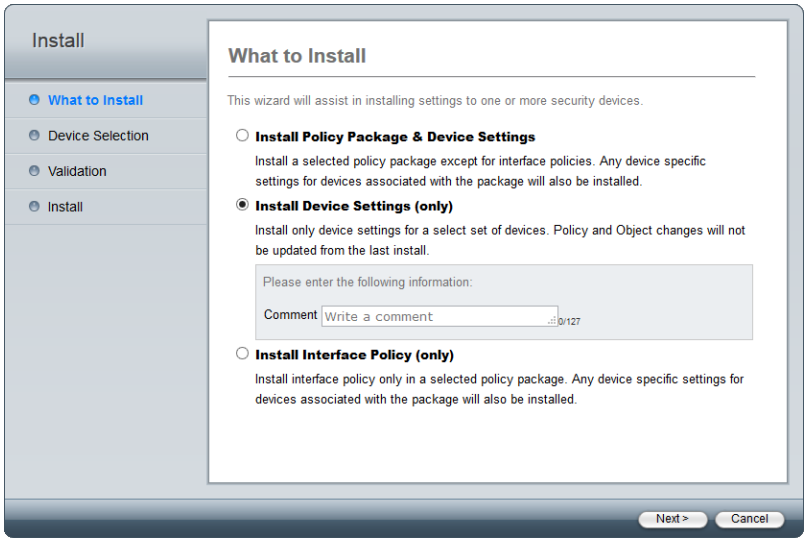
The installation phase displays the status of the installation process, and then lists the devices onto which the settings were installed and any errors or warning that occurred during the installation process.

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

Installing device settings (only)

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

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



Device selection

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

Validation

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

Installation

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

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

Installing interface policy (only)

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

Device selection

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

Validation

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

Installation

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

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

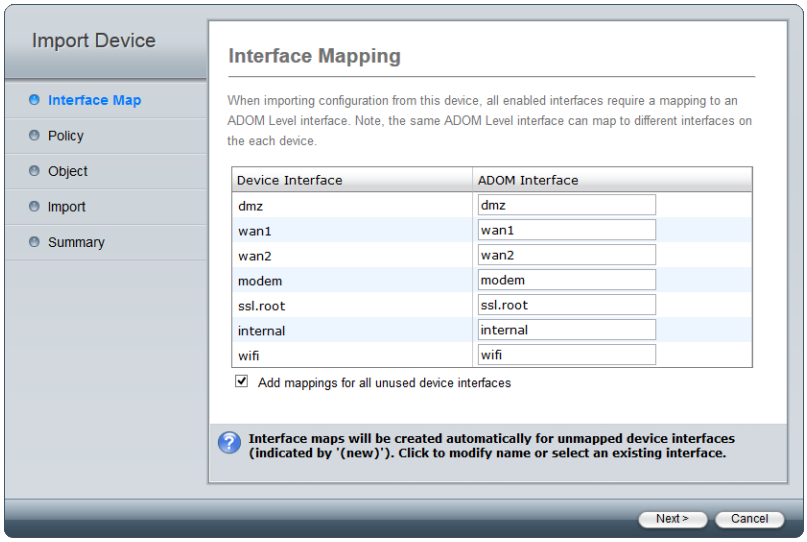
Import policy wizard

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 interface maps, policy databases, and objects.

Interface map

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

Interface maps will be created automatically for unmapped interfaces.



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

Policy

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

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

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

Object

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

Select *Next* to view the objects that are ready to be imported, then select *Next* again to proceed with importing.

Import

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

Summary

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

Re-install policy

Right-click on a device, and select *Re-install Policy* to re-install a policy package without launching the *Install wizard*. The option is disabled when the policy package is already synchronized.

You can also select *Install Config* from the right-click menu to install any device setting changes if the device is out of sync. This will only affect the settings for the selected device.

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

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. Select the FortiGate unit that you want to check the configuration status of. The device dashboard of for that unit is shown in the right content pane.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. Verify the status in the *Installation Tracking* section.
   The following information is shown:

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

Managing configuration revision history

In the *Device Manager* tab, select a device in the tree-menu. In the device dashboard *Configuration and Installation Status* widget, select *Revision History* in the *Total Revisions* row, to view the FortiManager repository.

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

configuration settings, compare different revisions, revert to previous settings, and download configuration files to a local computer.

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 216.
ID	A number assigned by the FortiManager system to identify the version of the configuration file saved in the FortiManager repository. Select an ID to view the configuration file. You can also select the Download button to save this configuration file from the FortiManager system to a local computer.
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 217 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 217.

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. In the content pane with a device already selected, go to the *Configuration and Installation Status* widget, in 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* in the *View Configuration* page. For more information.

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

1. In the content pane with a device already selected, go to the *Configuration and Installation Status* widget, in the *Total Revisions* row, select *Revision History*.
2. Select the *Name* for the version you want to change.
3. Type a name in the *Tag (Name)* field.
4. Optionally, type information in the *Comments* field.
5. Select *OK*.

Downloading and importing a configuration file

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

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

To download a configuration file to a local computer:

1. In the content pane with a device already selected, go to the *Configuration and Installation Status* widget, in the *Total Revisions* row, select *Revision History*.
2. Select the *ID* for the revision you want to download.
3. Select the *Download* button.
4. Select *Regular* or *Encrypted* download type. If you select *Encrypted Download*, type a password.
5. Select *OK*.
6. Specify a location to save the configuration file on the local computer.
7. Select *Save*.

To import a configuration file from a local computer:

1. In the content pane with a device already selected, go to the *Configuration and Installation Status* widget, in 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 type 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. In the content pane with a device already selected, go to the *Configuration and Installation Status* widget, in the *Total Revisions* row, select *Revision History*.
2. In 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:

To revert to another configuration file:

1. In the content pane with a device already selected, go to the *Configuration and Installation Status* widget, in the *Total Revisions* row, select *Revision History*.
2. Select the *Revert* icon for the revision you want to revert to.
3. Select *OK*.

Scripts

Scripts must be configured to be displayed to be accessible as described in this chapter. Go to *System Settings* > *Admin* > *Admin Settings* and select *Show Script* from the *Display Options on GUI* section to make it visible in the GUI. For more information, see Administrator settings on page 94.

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

FortiManager scripts enable you to create, execute, and view the results of scripts executed on FortiGate devices, policy packages, the ADOM database, the global policy package, or the DB. Scripts can also be filtered based on different device information, such as OS type and platform.

At least one FortiGate device must be configured in the FortiManager system for you to be able to use scripts.

Any scripts that are run on the global database must use complete commands. For example, if the full command is `config system global`, do not use `conf sys glob`.

Scripts can be written in one of two formats:

- A sequence of FortiGate CLI commands, as you would type them at the command line. A comment line starts with the number sign (#). A comment line will not be executed.
- Tcl scripting commands to provide more functionality to your scripts including global variables and decision structures.

When writing your scripts, it is generally easier to write them in a context-sensitive editor, and then cut and paste them into the script editor on your FortiManager system. This can help avoid syntax errors and can reduce the amount of troubleshooting required for your scripts.

For information about scripting commands, see the *FortiGate CLI reference*.

Before using scripts, ensure the `console-output` function has been set to `standard` in the FortiGate CLI. Otherwise, scripts and other output longer than a screen in length will not execute or display correctly.

When pushing a script from the FortiManager to the FortiGate with *workspace* enabled, you must save the changes in the *Policy & Objects* tab.

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 *Scripts* > *Script*. To configure script groups, go to *Scripts* > *CLI Script Group*. The script list for the selected ADOM will be displayed.

The following information is displayed:

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

The following options are available:

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

Run a script

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

Scripts can also be re-run from the script execution history by selecting the run button. See Script history on page 226 for information.

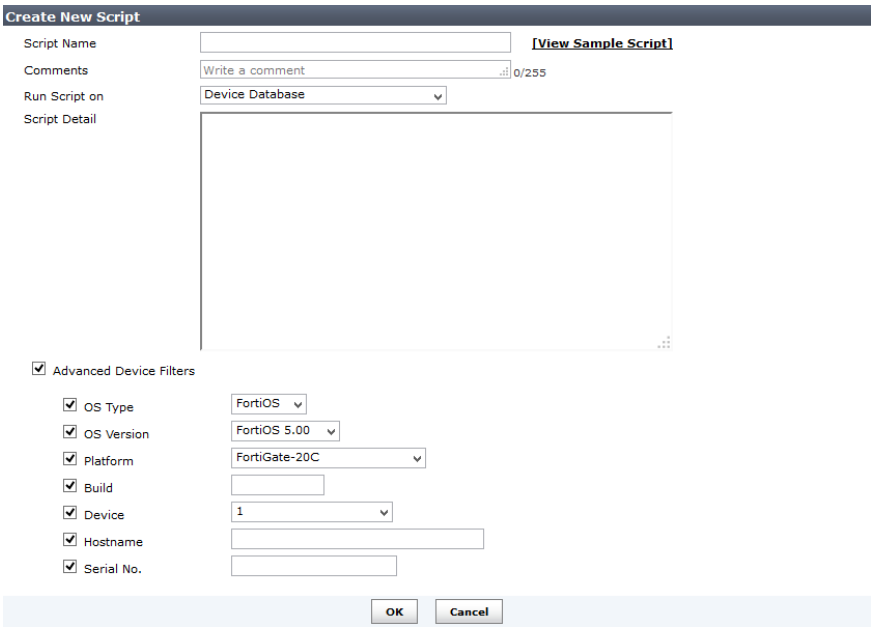
The *Execute Script* dialog box will open. This dialog box will vary depending on the script target. You will either be able to select a device or devices (left image below), or a policy package (right image).

3. Select to enable automatic execute type or create a recurring schedule for the script.
4. Select *OK* to run the script.
   The *Run Script* dialog box will open, showing the progress of the operation and providing information on its success or failure.
5. 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.
6. 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 menu, to open the *Create Script* dialog box.



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

Script Name	Type a unique name for the script.
View Sample Script	This option points to the FortiManager online help. Browse to the *Advanced Features* chapter to view sample scripts.
Comments	Optionally, type a comment for the script.
Run Script on	Select the script target. This settings will affect the options presented when you go to run a script. The options include: • *Device Database* • *Policy Package, ADOM Database* • *Remote FortiGate Directly (via CLI)*
Script Detail	Type the script itself, either manually using a keyboard, or by copying and pasting from another editor.
Advanced Device Filters	Select to adjust the advanced filters for the script. The options include: • *OS Type* (select from the drop-down list) • *OS Version* (select from the drop-down list) • *Platform* (select from the drop-down list) • *Build* • *Device* (select from the drop-down list) • *Hostname* • *Serial No.*

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

Edit a script

All of the same options are available when editing a script as when creating a new script, except the name of the script cannot be changed.

To edit a script, 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 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 menu.
   The *Clone Script* dialog box will open, showing the exact same information as the original, except *copy_* is appended to the script name.
3. Edit the script and its settings as needed and select *OK* to create the clone.

Delete a script

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

Export a script

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

To export a script:

1. 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 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.
3. Type a name for the script you are importing.
4. Optionally, type add a comment about the script.

5. Select the script target from the drop-down list.
6. Select *Browse* and locate the file to be imported on your local computer.
7. Select to add advanced device filters if required.
8. Select *OK* to import the script.

   If the script cannot be read, due to an incorrect file type or other issue, an error message will be displayed and the import process will be cancelled.

CLI script group

To create CLI script groups:

1. Go to *Scripts* > *CLI Script Group*.
2. Select *Create New* in the script action bar. The *Create New CLI Script Group(s)* page opens.
3. Configure the following settings:

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

4. Select OK to save the CLI script group.

Script syntax

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

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

Syntax applicable for address and address6

```
config firewall address
   edit xxxx

      ...regular FOS command here...

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

```
      next
   end
```

Syntax applicable for ippool and ippool6

```
config firewall ippool
   edit xxxx

      ...regular FOS command here...

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

Syntax applicable for vip, vip6, vip46, and vip64

```
config firewall vip
   edit xxxx

      ...regular FOS command here...

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

Syntax applicable for zone

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

Syntax applicable for local interface

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

```
      end
```

Syntax applicable for vpn tunnel

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

Syntax applicable for vpn console table

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

Syntax applicable for vpn console node

```
config vpnmgr node
   edit "1"
      set vpntable "<table_name>"
      set role hub|spoke
      set iface xxxx
      set hub_iface xxxx
      set automatic_routing enable|disable
      set extgw_p2_per_net enable|disable
      set banner xxxx
      set route-overlap use-old|use-new|allow
      set dns-mode manual|auto
      set domain xxxx
```

```
      set local-gw x.x.x.x
      set unity-support enable|disable
      set xauthtype disable|client|pap|chap|auto
      set authusr xxxx
      set authpasswd xxxx
      set authusrgrp xxxx
      set public-ip x.x.x.x
      config protected_subnet
         edit 1
            set addr xxxx xxxx ...
         next
      end
```

Syntax applicable for setting installation target on policy package

```
config firewall policy
   edit x

      ...regular policy command here...

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

Syntax applicable for global policy

```
config global header policy

   ...regular policy command here...

end

config global footer policy

   ...regular policy command here...

end
```

Script history

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

To view the script execution history:

1. In *Device Manager*, locate the device whose script history you want to view.
2. In the content pane, select *Dashboard*, and find the *Configuration and Installation Status widget*.
3. Select *View History* in the *Script Status* field of the widget to open the *Script Execution History table*.
4. To view the script history for a specific script, select the *Browse* icon in the far right column of the table to open the *Script History* dialog box.

5. To re-run a script, select the Run script now icon in the far right column of the table. The script is re-run. See Run a script on page 220.
6. Select *Return* to return to the device dashboard.

To view a script log:

1. Go to *System Settings* > *Task Monitor*.
2. Locate the script execution task whose log you need to view, and expand the task.
3. Select the *View Script Execution History* icon to open the script log window.
   For more information, see Task monitor on page 105.

Script samples

This section helps familiarize you with FortiManager scripts, provides some script samples, and provides some troubleshooting tips.

The scripts presented in this section are in an easy to read format that includes:

- the purpose or title of the script
- the script itself
- the output from the script (blank lines are removed from some output)
- any variations that may be useful
- which versions of FortiOS this script will execute on

Do not include `\r` in your scripts as this will cause the script to not process properly.

Script samples includes:

- CLI scripts
- Tcl scripts

CLI scripts

CLI scripts include only FortiOS CLI commands as they are entered at the command line prompt on a FortiGate device. CLI scripts do not include Tool Command Language (Tcl) commands, and the first line of the script is not “#!” as it is for Tcl scripts.

CLI scripts are useful for specific tasks such as configuring a routing table, adding new firewall policies, or getting system information. These example tasks easily apply to any or all FortiGate devices connected to the FortiManager system.

However, the more complex a CLI script becomes the less it can be used with all FortiGate devices - it quickly becomes tied to one particular device or configuration. One example of this is any script that includes the specific IP address of a FortiGate device’s interfaces cannot be executed on a different FortiGate device.

Samples of CLI scripts have been included to help get you started writing your own scripts for your network administration tasks.

Error messages will help you determine the causes of any CLI scripting problems, and fix them. For more information, see Error Messages on page 232.

The troubleshooting tips section provides some suggestions on how to quickly locate and fix problems in your CLI scripts. For more information, see Troubleshooting Tips on page 245.

CLI script samples

There are two types of CLI scripts. The first type is getting information from your FortiGate device. The second type is changing information on your FortiGate device.

Getting information remotely is one of the main purposes of your FortiManager system, and CLI scripts allow you to access any information on your FortiGate devices. Getting information typically involves only one line of script as the following scripts show.

To view interface information for port1:	
Script	`show system interface port1`

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

Variations	Remove the interface name to see a list that includes all the interfaces on the FortiGate device including virtual interfaces such as VLANs.
Note	This script does not work when run on a policy package.

	If the preceding script is used to be run on the FortiGate Directly (via CLI) or run on device database on a FortiGate has the VDOM enabled. The script will have be modified to the following:
	`config global`
	`  show system interface port1`
	`end`

	Since running on device database does not yield any useful information.
	View the log of script running on device: FortiGate-VM64-70
	`------- Executing time: 2013-10-15 13:27:32 ------`
	`Starting log (Run on database)`
	`config global`
	`end`
	`Running script on DB success`
	`------- The end of log ----------`

The script should be run on the FortiGate Directly (via CLI).
View the log of script running on device: FortiGate-VM64-70

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

To view the entries in the static routing table. To get any useful information, the script has to be re-written for the following if the VDOM is enabled for FortiGate and has to be run on the FortiGate Directly (via CLI).

```
config vdom
   edit root
      show route static
   next
end
```

Here is a sample run of the preceding script running on the FortiGate Directly (via CLI).
View the log of script running on device: FortiGate-VM64-70

```
------- Executing time: 2013-10-15 14:24:10 ------
Starting log (Run on device)
FortiGate-VM64 $ config vdom
FortiGate-VM64 (vdom) $ edit root
current vf=root:0
FortiGate-VM64 (root) $ show route static
config router static
   edit 1
      set device "port1"
      set gateway 10.2.0.250
   next
end
FortiGate-VM64 (root) $ next
FortiGate-VM64 (vdom) $ end
------- The end of log ----------
```

To view the entries in the static routing table:

Script

```
show route static
```

Output

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

Variations none

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

Script

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Running a CLI script on a FortiGate unit

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

```
        next
    end
```

- Running a CLI script on the global database

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

Error Messages

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

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

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

Troubleshooting Tips

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

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

Tcl scripts

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

Do not include the exit command that normally ends Tcl scripts; it will prevent the script from running.

This guide assumes you are familiar with the Tcl language and regular expressions, and instead focuses on how to use CLI commands in your Tcl scripts. Where you require more information about Tcl commands than this guide contains, please refer to resources such as the Tcl newsgroup, Tcl reference books, and the official Tcl website at http://www.tcl.tk.

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

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

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

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

To enable Tcl scripting, use the following CLI commands:

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

Limitations of FortiManager Tcl

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

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

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

Tcl variables

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

Example: Save system status information in an array.

Script:

```
#!
proc get_sys_status aname {
   upvar $aname a
puts [exec "# This is an example Tcl script to get the system status of the FortiGate\n"
    "# " 15 ]
   set input [exec "get system status\n" "# " 15 ]
# puts $input
   set linelist [split $input \n]
# puts $linelist
foreach line $linelist {
   if {![regexp {([^:]+):(.*)} $line dummy key value]} continue
      switch -regexp -- $key {
      Version {
      regexp {FortiGate-([^ ]+) ([^,]+),build([\d]+),.*} $value dummy a(platform) a
          (version) a(build)
   }
Serial-Number {
   set a(serial-number) [string trim $value]
}
   Hostname {
      set a(hostname) [string trim $value]
      } }
   }
}
get_sys_status status
puts "This machine is a $status(platform) platform."
puts "It is running version $status(version) of FortiOS."
puts "The firmware is build# $status(build)."
puts "S/N: $status(serial-number)"
puts "This machine is called $status(hostname)"
```

Output:

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

FortiGate-VM64 #

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

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

Variations:

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

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

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

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

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

In analyzing this script:

- line 1 is the required #! to indicate this is a Tcl script
- lines 2-3 open the procedure declaration
- lines 4-5 puts the output from the CLI command into a Tcl variable as a string, and breaks it up at each return character into an array of smaller strings
- line 6 starts a loop to go through the array of strings
- line 7 loops if the array element is punctuation or continues if its text
- line 8 takes the output of line 7's regular expression command and based on a match, performs one of the actions listed in lines 9 through 17
- lines 9-11 if regular expression matches 'Version' then parse the text and store values for the platform, version, and build number in the named array elements
- line 12-14 if regular expression matches 'Serial-Number' then store the value in an array element named that after trimming the string down to text only
- lines 15-17 is similar to line 12 except the regular expression is matched against 'Hostname'
- line 17-19 close the switch decision statement, the for each loop, and the procedure
- line 20 calls the procedure with an array name of status
- lines 21-25 output the information stored in the status array

Tcl loops

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

Example: Create 10 users from usr0001 to usr0010:

Script:

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

```
do_cmd "end"

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

Output:

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

------- Executing time: 2013-10-16 15:27:18 ------
Starting log (Run on device)
config vdom
FortiGate-VM64 (vdom) #
edit root
current vf=root:0
FortiGate-VM64 (root) #
config user local
FortiGate-VM64 (local) #
Adding user: usr0001
edit usr0001
new entry 'usr0001' added
FortiGate-VM64 (usr0001) #
set status enable
FortiGate-VM64 (usr0001) #
set type password
FortiGate-VM64 (usr0001) #
next

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

Variations:

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

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

In analyzing this script:

- line 1 is the required #! to indicate this is a Tcl script
- lines 2-4 open CLI command wrapper procedure
- line 5 declares the number of users to create
- line 6 gets the FortiGate ready for entering local users
- line 7 opens the for loop that will loop ten times
- line 8 sets the user name based on the incremented loop counter variable

- line 9 is just a comment to the administrator which user is being created
- lines 10-13 create and configure the user, leaving the CLI ready for the next user to be added
- line 14 ends the for loop
- line 15 ends the adding of users in the CLI
- line 16 executes a CLI command to prove the users were added properly

Tcl decisions

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

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

Example: Add information to existing firewall policies.

Script:

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

Variations:

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

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

In analyzing this script:

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

Additional Tcl Scripts

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

Script:

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

Output:

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

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

CPU states: 0% user 0% system 0% nice 90% idle
CPU0 states: 0% user 0% system 0% nice 90% idle
CPU1 states: 0% user 0% system 0% nice 90% idle
Memory states: 73% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes, 0 kbps in 30 minutes
Average sessions: 1 sessions in 1 minute, 2 sessions in 10 minutes, 2 sessions in 30
    minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second
    in last 10 minutes, 0 sessions per second in last 30 minutes
```

```
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 6 days, 1 hours, 34 minutes

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

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

Example: Configure common global settings.

Script:

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

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

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

```
fgt_cmd "unset $key"
}
}
fgt_cmd "end"
fgt_cmd "end"
#config system user group---end

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

Output:

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

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

Example: Configure syslogd settings and filters.

Script:

```
#!
#Run on FortiOS v5.00
#This script will configure log syslogd setting and
#filter
#key-value pairs for 'config log syslogd setting', no
#value means default value.
   set setting_list {{status enable} {csv enable}
```

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

Output:

```
Starting log (Run on device)

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

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

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

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

Script:

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

Output:

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

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

Script:

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

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

```
#config ips custom settings---begin
foreach rule_name [array names custom_rule] {
fgt_cmd "config ips custom"
fgt_cmd "edit $rule_name"
set_kv $custom_rule($rule_name)
fgt_cmd "end"
}
fgt_cmd "end"
#config ips custom settings---end
```

Output:

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

Variations:

None.

Tcl file IO

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

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

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

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

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

To write to a file:	

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

To read from a file:	

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

Output	`Hello, world!`

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

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

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

Both scripts close the file before they exit.

Troubleshooting Tips

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

- Make sure the commands you are trying to execute are valid for the version of FortiOS running on your target FortiGate device.
- You should always use braces when evaluating code that may contain user input, to avoid possible security breaches. To illustrate the danger, consider this interactive session:

```
% set userinput {[puts DANGER!]}
[puts DANGER!]
% expr $userinput == 1
DANGER!
0
% expr {$userinput == 1}
0
```

  In the first example, the code contained in the user-supplied input is evaluated, whereas in the second the braces prevent this potential danger. As a general rule, always surround expressions with braces, whether using expr directly or some other command that takes an expression.

- A number that includes a leading zero or zeros, such as 0500 or 0011, is interpreted as an octal number, not a decimal number. So 0500 is actually 320 in decimal, and 0011 is 9 in decimal.
- There is a limit to the number of scripts allowed on the FortiManager unit. Try removing an old script before trying to save your current one.
- Using the Tcl command “catch” you can add custom error messages in your script to alert you to problems during the script execution. When catch encounters an error it will return 1, but if there is no error it will return 0. For example:

```
if { [catch {open $someFile w} fid] } {
   puts stderr "Could not open $someFile for writing\n$fid"
   exit 1 ;# error opening the file!
   } else {
# put the rest of your script here
   }
```

Use Tcl script to access FortiManager’s device database or ADOM database

You can use Tcl script to access FortiManager’s device database or ADOM database (local database).

Example 1:

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

Syntax	`puts [exec_ondb "/adom/<adom_name>/pkg/<pkg_fullpath>" "embedded cli commands" "# "]`
Usage	`puts [exec_ondb "/adom/52/pkg/default" " config firewall address edit port5_address next end " "# "]`

Example 2:

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

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

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

Example 3:

Run Tcl script on a specific device in an ADOM:

Syntax	`puts [exec_ondb "/adom/<adom_name>/device/<dev_name>" "embedded cli commands" "# "]`
Usage	`puts [exec_ondb "/adom/v52/device/FGT60CA" " config global config system global set admintimeout 440 end end " "# "]`

Example 4:

Run Tcl script on all devices in an ADOM:

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

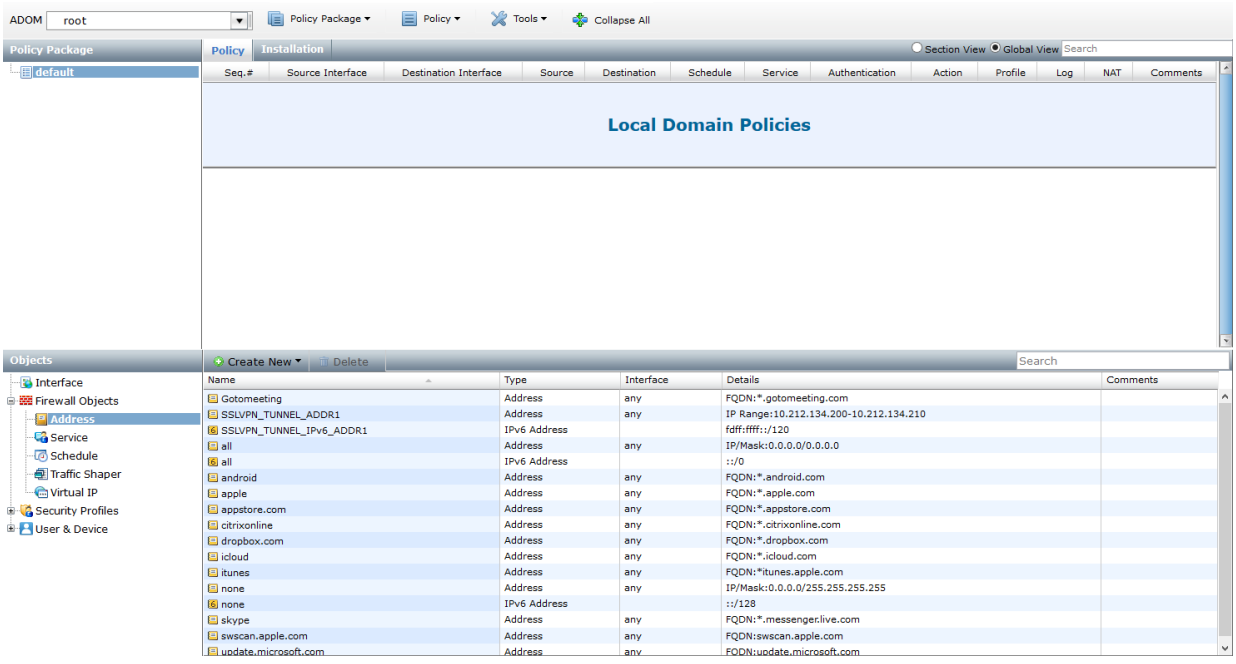
`exec_ondb` cannot be run on the Global ADOM.

Policy & Objects

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

If the administrator account you logged on with does not have the appropriate permissions, you will not be able to edit or delete settings, or apply any changes. Instead you are limited to browsing. To modify these settings, see Profile on page 86.

If workspace is enabled, all policies and objects are read-only until you lock the ADOM. After making any changes you must select the save icon. When unlocking the ADOM, before the save action has been select3ed, a warning message will open advising you that you have unsaved configuration changes. You can select to save the changes from the warning message dialog box. Alternatively, you can select to lock and edit a specific policy package in the ADOM.



The following options are available:

Policy Package	Select to access the policy package menu. The menu options are the same as the the right-click menu options.
Policy	Select to create a new policy.

Tools	Select and then select either *ADOM Revisions* or *Display Options* from the menu.
Collapse All / Expand All	Select to collapse or expand all policies.

In v5.0.5 and earlier, 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 36 for information on enabling or disabling workspace.

In v5.2.0 and later, if workspace is enabled, you can select to lock and edit the policy package in the right-click menu. You do not need to lock the ADOM first. The policy package lock status is displayed in the toolbar.

The following options are available:

Lock ADOM | Unlock ADOM	Select to lock or unlock the ADOM.
Sessions	Select to access the sessions menu. Select to save, submit, or discard changes made during the session.
Policy Package	Select to access the policy package menu. The menu options are the same as the the right-click menu options.
Policy	Select to create a new policy.
Tools	Select and then select either *ADOM Revisions* or *Display Options* from the menu. *ADOM Revisions* is not available when the ADOM is locked.
Collapse All | Expand All	Select to collapse or expand all policies.

About policies

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

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

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

Policy theory

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

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

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

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

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

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

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

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

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

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

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

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

Global policy packages

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

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

Global policy packages must be explicitly assigned to specific ADOMs to be used. When configuring global policies, a block of space in the policy table is reserved for *Local Domain Policies*. All of the policies in an ADOM's policy table 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*.

Policy workflow

An administrator will typically carry out two main functions with their devices through FortiManager: provisioning new devices or VDOMs on the network and managing the day-to-day operations of managed devices and VDOMs.

Provisioning new devices

There are multiple steps to provision a new device or VDOM to be managed by the FortiManager unit:

1. In the *Device Manager* tab, create a new VDOM or add a new device.
2. Assign a system template to the provisioned device (optional).
3. In the *Policy & Objects* tab, configure any dynamic objects you wish to assign to the new VDOM or device.
4. Determine how a policy will be defined for the new device: does the new device or VDOM have a new policy package unique to itself, or will use a package that is implemented elsewhere?
5. Run the *Install Wizard* to install any objects and policies for the new device, or create a new policy package.
6. If the new device uses an existing policy package, modify the installation targets of that package to include the new device and click the *Installation* tab.

Day-to-day management of devices

An administrator will often have to modify various objects for the devices they are responsible for managing. A typical set of tasks to manage an already provisioned device will include:

1. Adding, deleting, or editing various objects, such as firewall information, security profiles, user access rights, antivirus signatures, etc.
2. Adding, deleting, or editing all of the policy packages or individual policies within a policy package. This can include changing the order of operation, adding new policies, or modifying information or access permissions in the policy package.
3. Installing updates to devices.

Display options

The policy and objects that are displayed in the *Policy & Objects* page can be customized by selecting the *Tools* > *Display Options* menu option in the toolbar. Customizations are either per ADOM or at the global level.

The display and global level options in the GUI are dependent on the ADOM version. These display options will vary from one ADOM to another.

Turn the various options on or off (visible or hidden) by clicking the on/off button next to feature name. Turn all of the options in a category on by selecting *All On* under the category name, or turn all of the categories on by selecting *All On* at the bottom of the window.

Various display options are enabled by default and cannot be turned off.

Once turned on, the corresponding options settings will be configurable from the appropriate location in the *Policy & Objects* tab.

Reset all of the options by selecting *Reset* at the bottom of the screen, or reset only the options in a category by selecting *Reset* under the category name.

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 94 for more information.

Lock an ADOM or policy package

If workspace is enabled, you must lock an ADOM/Policy Package prior to performing any management tasks on it. For more information, see Concurrent ADOM access on page 36.

To lock an ADOM:

1. Select the specific ADOM on which you will be making changes from the drop-down list in the toolbar, or select *Global*.
2. Select the lock icon next to the drop-down list 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, unless lock override is enabled (see Extend workspace to entire ADOM on page 35).

To lock a policy package:

1. Select the specific ADOM on which you will be making changes from the drop-down list in the toolbar, or select *Global*.
2. Select the policy package, click the right mouse button, and select *Lock & Edit* from the menu.

   The policy package will now be locked, allowing you to make changes to it, and preventing other administrators from making any changes, unless lock override is enabled (see Extend workspace to entire ADOM on page 35).

When the policy package is locked, other users are unable to lock the ADOM. The policy package can be edited in a private workspace. Only the policy package is in the workspace, not the object database. When locking and editing a policy package, the object database remains locked. The policy package lock status is displayed in the tool-bar.

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. Select a policy package and click the right mouse button on a policy package to access the menu. Alternatively, select the *Policy Package* menu in the toolbar.
3. Under the *Policy Folder* heading in the menu, select *Create New*.
4. Type a name for the new policy folder in the dialog box and then select *OK*. The new policy folder will be added to the tree menu.

You can create new policy folders within existing policy folders to help you better organ-ize your policy packages. Drag the policy package to the policy folder.

To create a new global policy package:

1. Select *Global* in the toolbar.
2. Right-click on a policy package then, under the *Global Policy Package* heading, select *Create New*.
3. Type a name for the new global policy package in the dialog box. If you are cloning a previous policy package, select *Clone Policy Package* and type the name of the policy package you would like to clone in the resulting text field.
4. 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, or select the *Policy Package* menu in the toolbar.
3. Under the *Policy Package* heading in the menu, select *Create New*. The *Create New Policy Package* dialog box opens.
4. Configure the following settings:

Name	Type a name for the new policy package
Clone Policy Package	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.

5. Select *OK* to add the policy package.
6. Select *Installation* in the Policy Package tab bar then select *Add* in the toolbar. The *Add Device/Group to Policy Package Installation Target* window opens.
7. Select the devices or groups for the policy package.
8. Select *OK* to save the setting.

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 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 menu. Type the new name for the global policy package or policy package folder in the dialog box and select *OK*.

To rename a local policy package, right-click on the policy package and select *Rename*. Type the new name (or edit the current name) in the *Name* field of the *Rename* 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* from the drop-down ADOM list and select the policy package in the *Global Policy Package* tree menu.
2. Select *Assignment* in the Policy Package tab bar to view the ADOM assignment list.
3. If required, select *Add ADOM* from the content toolbar to add an ADOM to the assignment 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 content toolbar. The *Assign* dialog box opens.
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.

In the *Assignment* tab you can also select to edit the ADOM list, delete ADOM from the list, assign and unassign 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 menu, select *Install Wizard*. The install wizard opens.
4. Follow the steps in the install wizard to install the policy package. You can select to install policy package and device settings or install the interface policy only.

   For more information on the install wizard, see Install wizard on page 208. For more information on editing the installation targets, see Edit the installation targets for a policy package on page 256.

Reinstall a policy package

To reinstall 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 menu, select *Re-install*. The policy package will be reinstalled to the target device.

Schedule a policy package install

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

Select the clock icon which is displayed beside the policy package name to create an install schedule. Select this icon to edit or cancel the schedule. When a scheduled install has been configured and is active, hover the mouse over the icon to view the scheduled date and time.

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

1. Select the ADOM that contains the policy package that you are installing from the drop-down list in the toolbar.
2. Right-click on a policy package in the *Policy Package* tree.
3. Under the *Policy Package* heading in the menu, select *Install Wizard*. The *Install* wizard will open.
4. Select *Install Policy Package & Device Settings*.
5. Enable *Schedule Install*, and set the install schedule date and time.
6. Select *Next*. In the device selection screen edit the installation targets as required.
7. Select *Next*. In the interface validation screen edit the interface mapping as required.
8. Select *Schedule Install* to continue to the policy and object validation screen. In the ready to install screen you can copy the log and download the preview text file.

To edit or cancel an install schedule:

1. Select the ADOM that contains the policy package whose schedule you are editing or canceling from the drop-down list in the toolbar.
2. Click the clock icon next to the policy package name in the *Policy Package* tree. The *Edit Install Schedul*e dialog box will be displayed.
3. Select *Cancel Schedule* to cancel the install schedule, then select *OK* in the confirmation dialog box to cancel the schedule. Otherwise, edit the install schedule as required and select *OK* to save your changes.

Export a policy package

You can export a policy package to a CSV file.

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 menu, select *Export*.
4. 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 ADOM that contains the policy package whose installation target you are editing from the drop-down list in the toolbar.
2. Select the name of the policy package from the list, then select the *Installation* tab in the policy package toolbar.
3. Select *Add* in the toolbar. The *Add Installation Target* dialog box opens.
4. Adjust the installation targets as required, then select *OK*.

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.

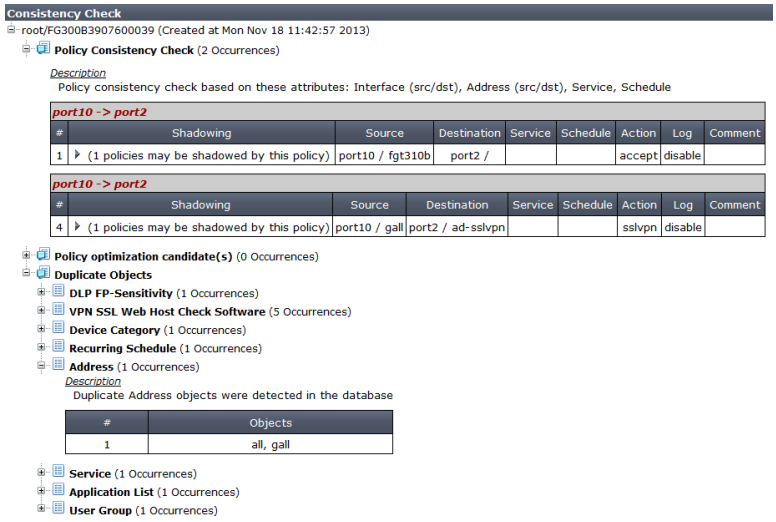
The policy check uses an algorithm to evaluate policy objects, based on the following attributes:

- 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 ADOM that you will be performing the consistency check on 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, select *Policy Check*. The *Consistency Check* dialog box opens.
4. To perform a new consistency check, select *Perform Policy Consistency Check*, then select *Apply*.
   A policy consistency check is performed, and the results screen is shown.



To view the results of the last policy consistency check:

1. Select the ADOM that you previously performed a consistency check in 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 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.

Policy search

Use the search field in the *Policy & Objects* tab to search policies for matching rules or objects. Entering text in the search field will highlight matches.

Managing policies

Policies in policy packages can be created and managed by selecting an ADOM from the drop-down list, and then selecting the policy package whose policies you are configuring from the policy package list. Sections can also be added to the policy list to help organize your policies.

The content pane contains tabs for configuring different policy types, targets, and NAT entries. *Policy* and *Installation* are enabled by default in *Display Options*; see Display options on page 252 for more information.

- Policy
- Interface policy
- Central NAT
- IPv6 policy
- Explicit proxy policy
- IPv6 interface policy
- DoS policy
- IPv6 DoS policy
- NAT46 policy
- NAT64 policy
- Installation

Various options are also available from column specific right-click menus, for more information see Column options on page 276.

If workspace is enabled, you must lock an ADOM or policy package prior to performing any management tasks on it. See Lock an ADOM or policy package on page 252 for instructions.

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

Not all policy and object options are enabled by default. To configure the enabled options, select *Display Options* in the toolbar.

Section view will be disabled if one or more policies are using the *Any* interface, or if one or more policies are configured with multiple source or destination interfaces.

To create a new policy:

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

Please see the section below that corresponds to the type of policy you are creating for specific instructions on creating that type of policy.

Policy creation will vary by ADOM version.

To insert a policy:

Generic policies can be inserted above or below the currently selected policy by right-clicking within the sequence number cell and selecting *Insert Policy* > *Above* or *Insert Policy* > *Below* from the menu.

To edit a policy:

Policies can be edited by either right-clicking on the policy sequence number in the policy list and selecting *Edit* in the menu, or by double clicking on the sequence number. Both methods will open the *Edit Policy* dialog box.

Policies can also be edited in-line by right-clicking on either the cell that is to be edited or on the content within that cell.

To clone a policy:

To clone a policy, right-click in the policy sequence number cell and select *Clone* from the menu. The *Clone Policy* dialog box opens with all of the settings of the original policy. Edit the settings as required and select *OK* to create the clone.

To copy, cut, or paste a policy:

Policies can be copied and cut using the requisite selection from the menu found by right-clicking in the policy sequence number cell.

When pasting a copied or cut policy, it can be inserted above or below the currently selected policy.

The menu also provides the option to *Cancel Copy/Cut* in the event that you need to undo the copy or cut that you just performed.

To delete a policy:

To delete a policy, right-click in the policy sequence number cell and select *Delete* from the menu. Select *OK* in the confirmation dialog box to delete the policy.

To add a section:

Sections can be used to help organize your policy list. Policies can also be appended to sections.

To add a section, right-clicking in the sequence number cell and select *Add Section* > *Above* or *Add Section* > *Below* to add a section either above or below the currently selected policy.

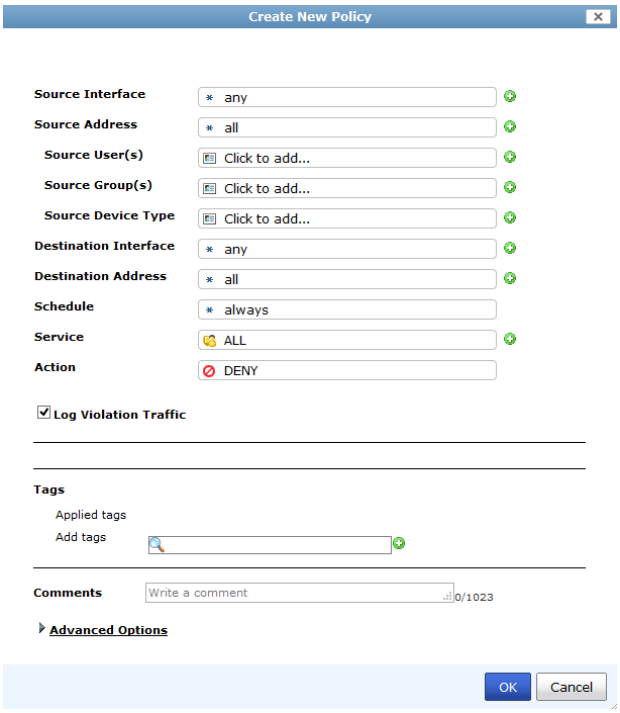
Policy

The section describes how to create a new IPv4 policy.

The following instructions are specific to FortiOS v5.2 ADOMs. For information on creating policies in v5.0 ADOMs, see the *FortiOS Handbook*, available in the Fortinet Document Library.

To create a new IPv4 policy:

1. Select the ADOM from the drop-down list in the toolbar.
2. Select the policy package where you will be creating the new policy from the tree menu.
3. Right-click on the sequence number of a current policy, or in an empty area of the content pane, and select *Create New* from the menu.
4. If you are creating a global policy, select *Create New* > *Header Policy* or *Create New* > *Footer Policy*. The *Create New Policy* dialog box opens.



5. Enter the following information:

Source Interface	Select the source interface. Select the add icon to add multiple values for this field. Select the remove icon to remove values.
Source Address	Select to add source addresses or address groups.Select the add icon to add multiple values for this field. Select the remove icon to remove values. Addresses and address groups can also be created by selecting *Create New* in the dialog box. See Create a new object on page 291 for more information.
Source User(s)	Select source users. Select the add icon to add multiple values for this field. Select the remove icon to remove values. This option is only available if the *Action* is set to *ACCEPT* or *DENY*.
Source Groups(s)	Select source groups. Select the add icon to add multiple values for this field. Select the remove icon to remove values. This option is only available if the *Action* is set to *ACCEPT* or *DENY*.
Source Device Type	Select device types. Select the add icon to add multiple values for this field. Select the remove icon to remove values. This option is only available if the *Action* is set to *ACCEPT* or *DENY*.

Destination Interface	Select the destination interface. Select the add icon to add multiple values for this field. Select the remove icon to remove values.
Destination Address	Select to add destination addresses or address groups. Select the add icon to add multiple values for this field. Select the remove icon to remove values. Addresses, address group, virtual IP, and virtual IP groups can also be created by selecting *Create New* in the dialog box. See Create a new object on page 291 for more information.
Schedule	Select a schedule or schedules for the policy. Schedules (one time, recurring, and schedule group) can also be created by selecting *Create New* in the dialog box. See Create a new object on page 291 for more information.
Service	Select services or service groups for the policy. Select the add icon to add multiple values for this field. Select the remove icon to remove values. Services and service groups can also be created by selecting *Create New* in the dialog box. See Create a new object on page 291 for more information.
Action	Select an action for the policy to take, whether *ACCEPT*, *DENY*, or *IPSEC*.
NAT	Select to enable NAT. If enabled, select *Use Destination Interface Address* (with or without *Fixed Port*) or *Dynamic IP Pool* (select the pool from the list, or a new pool can be created). This option is only available if the *Action* is set to *ACCEPT*.
Compliant with Endpoint Profile	Select to enforce compliance with the FortiClient Profile. This option is only available when selecting to add a device type to the *Source Device Type* field.
Logging Options	Select one of the following options: • *No Log* • *Log Security Events* • *Log All Sessions* When *Log All Sessions* is selected, you can select to generate logs when the session starts and to capture packets. This option is only available if the *Action* is set to *ACCEPT*.
Log Violation Traffic	Select to log violation traffic. This option is only available if the *Action* is set to *DENY*.
Enable Web Cache	Select to enable web cache. This option is only available if the *Action* is set to *ACCEPT*.

Enable WAN Optimization	Select to enable WAN optimization. If enabled, select *active* or *passive* from the drop down list, and select a profile to use for the optimization. This option is only available if the *Action* is set to *ACCEPT*.
Certificate	Select the certificate from the drop-down list. This option is only available if the *Action* is set to *ACCEPT*.
Customize Authentication Messages	Select the authentication message from the drop-down list. This option is only available if the *Action* is set to *ACCEPT*.
Resolve User Names Using FSSO Agent	Select to enable this feature. This option is only available if the *Action* is set to *ACCEPT*.
Enable Disclaimer	Select to enable the disclaimer, and type the redirect URL. This option is only available if the *Action* is set to *ACCEPT*.
VPN Tunnel	Select the VPN from the drop down list. Select to allow traffic to be initiated from the remote site. This option is only available if the *Action* is set to *IPSEC*.
Security Profiles	This option is only available if the *Action* is set to *ACCEPT* or *IPSEC*.
Enable AntiVirus	Select to enable antivirus and select the profile from the drop-down list.
Enable Web Filter	Select to enable Web Filter and select the profile from the drop-down list.
Enable Application Control	Select to enable Application Control and select the profile from the drop-down list.
Enable IPS	Select to enable IPS and select the profile from the drop-down list.
Enable Email Filter	Select to enable Email Filter and select the profile from the drop-down list.
Enable DLP Sensor	Select to enable DLP Sensor and select the profile from the drop-down list.
Enable VoIP	Select to enable VoIP and select the profile from the drop-down list.
Enable ICAP	Select to enable ICAP and select the profile from the drop-down list.
Enable SSL/SSH Inspection	This feature is enabled by default. Select the profile from the drop-down list.
Proxy Options	Select to enable Proxy Options and select the profile from the drop-down list. This option is only available when *Web Filter*, *Email Filter*, or *DLP Sensor* is enabled.
Traffic Shaping	Select to enable traffic shaping and select the traffic shaper object from the drop-down list. These options are only available if the *Action* is set to *ACCEPT* or *IPSEC*.

Reverse Direction Traffic Shaping	Select to enable reverse direction traffic shaping and select the traffic shaper object from the drop-down list.
Per-IP Traffic Shaping	Select to enable per-IP traffic shaping and select the traffic shaper object from the drop-down list. This option is only available if the *Action* is set to *ACCEPT* or *IPSEC*.
Tags	View the tags currently applied to the policy and add new tags.
Comments	Type a comment.
Advanced Options	For more information on advanced option, see the *FortiOS CLI Reference*. The available options are dependent on the policy action.
auth-path	Enable or disable authentication-based routing.
auth-redirect-addr	HTTP-to-HTTPS redirect address for firewall authentication.
auto-asic-offload	Enable or disable policy traffic ASIC offloading.
captive-portal-exempt	Enable or disable exemption of captive portal.
custom-log-fields	Select the custom log fields from the drop-down list.
diffserv-forward	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic.
diffserv-reverse	Enable or disable application of the DSCP value to the DSCP field of reverse (reply) traffic. If enabled, also configure `diffservcode-rev`.
diffservcode-forward	Type the DSCP value that the FortiGate unit will apply to the field of originating (forward) packets. The value is 6 bits binary. The valid range is 000000-111111.
diffservcode-rev	Type the DSCP value that the FortiGate unit will apply to the field of reply (reverse) packets. The value is 6 bits binary. The valid range is 000000-111111.
fall-through-unauthenticated	Enable to allow an unauthenticated user to skip authentication rules and possibly match another policy.
fsso-agent-for-ntlm	Select the FSSO agent for NTLM from the drop-down list.
log-unmatched-traffic	Enable or disabling logging dropped traffic for policies with `identity-based` enabled.
match-vip	Enable or disable match DNATed packet.
natip	Type the NAT IP address in the text field.
ntlm-enabled-browsers	Type a value in the text field.

ntlm-guest	Enable or disable NTLM guest.
permit-any-host	Enable to accept UDP packets from any host.
permit-stun-host	Enable to accept UDP packets from any STUN host.
profile-type	Select the profile type from the drop-down list.
rtp-addr	Select the RTP address from the drop-down list.
rtp-nat	Enable to apply source NAT to RTP packets received by the firewall policy.
schedule-timeout	Enable to force session to end when policy schedule end time is reached.
send-deny-packet	Enable to send a packet in reply to denied TCP, UDP or ICMP traffic.
session-ttl	Type a value for the session time-to-live (TTL) from 300 to 604800, or type 0 for no limitation.
tcp-mss-receiver	Type a value for the receiver's TCP MSS.
tcp-mss-sender	Type a value for the sender's TCP MSS.
timeout-send-rst	Enable sending a TCP reset when an application session times out.
transaction-based	Enable or disable this feature.
vlan-cos-fwd	Type the VLAN forward direction user priority.
vlan-cos-rev	Type the VLAN reverse direction user priority.
wccp	Enable or disable Web Cache Communication Protocol (WCCP).
webcache-https	Enable or disable web cache for HTTPS.

6. Select *OK* to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number.

Interface policy

The *Interface Policy* tab allows you to create, edit, delete, and clone interface policies. The following information is displayed for these policies: Seq.#, Interface (source interface), Source (source address), Destination (destination address), Service, IPS Sensor (profile), Application Sensor (profile), AntiVirus (profile), Web Filter (profile), DLP Sensor (profile), Email Filter (profile), and Install On (installation targets).

Select Display Options in the Policy & Objects tab, and click the Interface Policy switch to display this option in the Policy Package tab bar.

The following instructions are specific to FortiOS v5.2 ADOMs. For information on creating policies in v5.0 ADOMs, see the *FortiOS Handbook*, available in the Fortinet Document Library.

To create a new interface policy:

1. Select the ADOM from the drop-down list in the toolbar.
2. Select the policy package where you are creating the new identity policy from the tree menu.
3. Select *Interface Policy* in the policy toolbar.
4. Right-click on the sequence number of a current policy, or in an empty area of the content pane and select *Create New* from the menu. The *Create New Policy* dialog box opens.
5. Configure the following settings:

Source Interface		Select the source zone from the drop-down list.
Source Address		Select the source address from the drop-down list. You can create a new address or address group in the *Add Source Address* window. Select the add icon to add multiple values for this field. Select the remove icon to remove values.
Destination Address		Select the destination address from the drop-down list. You can create a new address or address group in the *Add Destination Address* dialog box. Select the add icon to add multiple values for this field. Select the remove icon to remove values.
Service		Select the service from the drop-down list. You can create a new service or service group in the *Add Service* dialog box. Select the add icon to add multiple values for this field. Select the remove icon to remove values.
	Enable AntiVirus	Select to enable antivirus and select the profile from the drop-down list.
	Enable Web Filter	Select to enable Web Filter and select the profile from the drop-down list.
	Enable Application Control	Select to enable Application Control and select the profile from the drop-down list.
	Enable IPS	Select to enable IPS and select the profile from the drop-down list.
	Enable Email Filter	Select to enable Email Filter and select the profile from the drop-down list.
	Enable DLP Sensor	Select to enable DLP Sensor and select the profile from the drop-down list.
Advanced Options		
	address-type	The default value for this field is `ipv4`.
	logtraffic	Enable or disable interface log traffic

6. Select *OK* to save the setting.
   You can enable or disable the policy using the right-click menu.

Central NAT

The central NAT table enables you to define and control (with more granularity) the address translation performed by the FortiGate unit. With the NAT table, you can define the rules which dictate the source address or address group, and which IP pool the destination address uses.

While similar in functionality to IP pools, where a single address is translated to an alternate address from a range of IP addresses, with IP pools there is no control over the translated port. When using the IP pool for source NAT, you can define a fixed port to guarantee the source port number is unchanged. If no fixed port is defined, the port translation is randomly chosen by the FortiGate unit. With the central NAT table, you have full control over both the IP address and port translation.

The FortiGate unit reads the NAT rules in a top-down methodology, until it hits a matching rule for the incoming address. This enables you to create multiple NAT policies that dictate which IP pool is used based on the source address. The NAT policies can be rearranged within the policy list as well. NAT policies are applied to network traffic after a security policy.

The Central NAT tab allows you to create, edit, delete, and clone central NAT entries. The following information is displayed for these entries: *NAT ID*, *Status*, *Original Address*, *Original Source Port*, *Translated Address*, *Translated Port*, and *Last Modified* (administrator, and date and time that the entry was last modified). Select the checkbox in the *Status* column to enable or disable the central NAT entry.

Select *Display Options* in the *Policy & Objects* tab, then click the *Central NAT* switch to display this option in the Policy Package tab bar.

The following instructions are specific to FortiOS v5.2 ADOMs. For information on creating Central NAT tables in v5.0 ADOMs, see the *FortiOS Handbook*, available in the Fortinet Document Library.

Central NAT does not support *Section View*.

To create a new central NAT entry:

1. Select the ADOM from the drop-down list in the toolbar.
2. Select the policy package where you are creating the new interface policy from the tree menu.
3. Select *Central NAT* in the policy toolbar.
4. Select *Create New* from the toolbar. The *New NAT* page opens.
5. Configure the following settings:

Source Address	Select the source address from the drop-down list. You can select to create a new address or address group in the *Source Address* dialog box.
Translated Address	Select the translated address from the drop-down list. You can select to create a new IP Pool in the *Translated Address* dialog box.
Original Source Port	Type the original source port range.
Translated Port	Type the translated port range.

6. Select *OK* to save the setting.

IPv6 policy

IPv6 security policies are created both for an IPv6 network, and a transitional network. A transitional network is a network that is transitioning over to IPv6, but must still have access to the Internet or must connect over an IPv4 network.

These policies allow for this specific type of traffic to travel between the IPv6 and IPv4 networks. The IPv6 options for creating these policies is hidden by default.

To create a new IPv6 Policy, go to the *Policy & Objects* tab and select *IPv6 Policy* in the policy toolbar. Right-click the content pane and select *Create New* > *Policy* or *Create New* > *Identity Policy*. See Policy on page 259 for more information.

Select *Display Options* in the *Policy & Objects* tab, and click the *IPv6 Policy* switch to display this option in the Policy Package tab bar.

Section view will be disabled if one or more policies are using the '*Any*' interface, or one or more policies are configured with multiple source or destination interfaces.

Explicit proxy policy

For information on creating explicit proxy policies in FortiManager v5.2, see the *FortiOS Handbook* available in the Fortinet Document Library.

Select *Display Options* in the *Policy & Objects* tab, and click the *Explicit Proxy Policy* switch to display this option in the Policy Package tab bar.

IPv6 interface policy

To create a new IPv6 Interface Policy, go to the *Policy & Objects* tab and select *IPv6 Interface Policy* in the policy toolbar. Right-click the content pane and select *Create New*. See Interface policy on page 264 for more information.

Select *Display Options* in the *Policy & Objects* tab, and click the *IPv6 Interface Policy* switch to display this option in the Policy Package tab bar.

For information on creating policies in v5.2, see the *FortiOS Handbook* available in the Fortinet Document Library.

DoS policy

The DoS (Denial of Service) Policy tab allows you to create, edit, delete, and clone DoS policies. The following information is displayed for these policies: *Seq.#* (sequence number), *Interface* (incoming interface), *Source* (source address), *Destination* (destination address), *Service*, and *Install On* (installation targets).

Select *Display Options* in the *Policy & Objects* tab, and click the *DoS Policy* switch to display this option in the Policy Package tab bar.

The following instructions are specific to FortiOS v5.2 ADOMs. For information on creating policies in v5.0 ADOMs, see the *FortiOS Handbook*, available in the Fortinet Document Library.

To create a DoS policy:

1. Select the ADOM from the drop-down list in the toolbar.
2. Select the policy package where you are creating the new DoS policy from the tree menu.
3. Select *DoS Policy NAT* in the policy toolbar.
4. Right-click on the sequence number of a current policy, or in an empty area of the content pane and select *Create New* from the menu. The *Create New Policy* dialog box opens.
5. Configure the following settings:

Incoming Interface	Select the incoming interface from the drop-down list.
Source Address	Select the source address from the drop-down list. You can select to create a new address or address group in the *Source Address* dialog box.
Destination Address	Select the destination address from the drop-down list. You can create a new address or address group in the *Add Destination Address* dialog box.
Service	Select the service from the drop-down list. You can create a new service or service group in the *Add Service* dialog box.
tcp_syn_flood	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. |The default threshold is 2000.
tcp_port_scan	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 1000.
tcp_src_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
tcp_dst_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
udp_flood	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 2000.
udp_scan	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 2000.

udp_src_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
udp_dst_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
icmp_flood	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 250.
icmp_sweep	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 100.
icmp_src_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 300.
icmp_dst_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 1000.
ip_src_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
ip_dst_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
scttp_flood	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 2000.
sctp_scan	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 1000.
sctp_src_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
sctp_dst_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.

6. Select *OK* to save the setting.

IPv6 DoS policy

The IPv6 DoS Policy tab allows you to create, edit, delete, and clone IPv6 DoS policies. For more information on configuring DoS policies, see DoS policy on page 267.

Select *Display Options* in the *Policy & Objects* tab, and click the *IPv6 DoS Policy* switch to display this option in the Policy Package tab bar.

NAT46 policy

Use NAT46 policies for IPv6 environments where you want to expose certain services to the public IPv4 Internet. You will need to configure a virtual IP to permit the access. The NAT46 Policy tab allows you to create, edit, delete, and clone NAT46 policies.

The following instructions are specific to FortiOS v5.2 ADOMs. For information on creating policies in v5.0 ADOMs, see the *FortiOS Handbook*, available in the Fortinet Document Library.

Select *Display Options* in the *Policy & Objects* tab, and click the *NAT46 Policy* switch to display this option in the Policy Package tab bar.

To create a NAT46 policy:

1. Select the ADOM from the drop-down list in the toolbar.
2. Select the policy package where you are creating the new NAT46 policy from the tree menu.
3. Select *NAT46 Policy* in the policy toolbar.
4. Right-click on the sequence number of a current policy, or in an empty area of the content pane and select *Create New* from the menu. The *Create New Policy* dialog box opens.
5. Configure the following settings:

Source Interface	Select the source interface from the drop-down list.
Source Address	Select the source address from the drop-down list. You can select to create a new address or address group in the *Source Address* dialog box.
Destination Interface	Select the destination interface from the drop-down list.
Destination Address	Select the destination address from the drop-down list. You can create a new address or address group in the *Add Destination Address* dialog box.
Schedule	Select a schedule or schedules for the policy. Schedules can also be created by selecting *Create New* in the dialog box. See Create a new object on page 291 for more information.
Service	Select the service from the drop-down list. You can create a new service or service group in the *Add Service* dialog box.
Action	Select an action for the policy to take, whether *ACCEPT* or *DENY*. When *Action* is set to *Accept*, you can configure *NAT* and *Traffic Shaping*.
Log Allowed Traffic **Log Violation Traffic**	Select to log allowed traffic/violation traffic. This setting is dependent on the *Action* setting.

NAT		NAT is enabled by default for this policy type.
	Use Destination Interface Access	Select to use the destination interface address. This setting is enabled by default.
	Fixed Port	Select to enable fixed port.
Traffic Shaping		Select to enable traffic shaping and select a default or custom traffic shaper object from the drop-down list.
	Reverse Direction Traffic Shaping	Select to enable reverse direction traffic shaping and select a default or custom traffic shaper object from the drop-down list.
Per-IP Traffic Shaping		Select to enable per-IP traffic shaping and select the related object from the drop-down list.
Tags		You can add tags for tag management. Type a tag in the text field and select the add icon to apply the tag to the policy.
Comments		Type optional comments for the policy.
Advanced		
	permit-any-host	Enable to accept UDP packets from any host.
	tcp-mss-receiver	Type a value for the receiver's TCP MSS.
	tcp-mss-sender	Type a value for the sender's TCP MSS.

6. Select *OK* to save the policy.

NAT64 policy

Use NAT64 policies to perform network address translation (NAT) between an internal IPv6 network and an external IPv4 network. The NAT64 Policy tab allows you to create, edit, delete, and clone NAT64 policies.

Select *Display Options* in the *Policy & Objects* tab, and click the *NAT64 Policy* switch to display this option in the Policy Package tab bar.

The following instructions are specific to FortiOS v5.2 ADOMs. For information on creating policies in v5.0 ADOMs, see the *FortiOS Handbook*, available in the Fortinet Document Library.

To create a NAT64 policy:

1. Select the ADOM from the drop-down list in the toolbar.
2. Select the policy package where you are creating the new NAT64 policy from the tree menu.
3. Select *NAT64 Policy* in the policy toolbar.
4. Right-click on the sequence number of a current policy, or in an empty area of the content pane and select *Create New* from the menu. The *Create New Policy* dialog box opens.

5. Configure the following settings:

Source Interface	Select the source interface from the drop-down list.
Source Address	Select the source address from the drop-down list. You can select to create a new address or address group in the *Source Address* dialog box.
Destination Interface	Select the destination interface from the drop-down list.
Destination Address	Select the destination address from the drop-down list. You can create a new address or address group in the *Add Destination Address* dialog box.
Schedule	Select a schedule or schedules for the policy. Schedules can also be created by selecting *Create New* in the dialog box. See Create a new object on page 291 for more information.
Service	Select the service from the drop-down list. You can create a new service or service group in the *Add Service* dialog box.
Action	Select an action for the policy to take, whether *ACCEPT* or *DENY*. When *Action* is set to *Accept*, you can configure *NAT* and *Traffic Shaping*.
Log Allowed Traffic **Log Violation Traffic**	Select to log allowed traffic/violation traffic. This setting is dependent on the *Action* setting.
NAT	NAT is enabled by default for this policy type.
Use Destination Interface Access	Select to use the destination interface address.
Fixed Port	Select to enable fixed port.
Dynamic IP Pool	Select to enable dynamic IP pool and select the dynamic IP pool from the drop-down list.
Traffic Shaping	Select to enable traffic shaping and select a default or custom traffic shaper object from the drop-down list.
Reverse Direction Traffic Shaping	Select to enable reverse direction traffic shaping and select a default or custom traffic shaper object from the drop-down list.
Per-IP Traffic Shaping	Select to enable per-IP traffic shaping and select the related object from the drop-down list.
Tags	You can add tags for tag management. Type a tag in the text field and select the add icon to apply the tag to the policy.
Comments	Type optional comments for the policy.

6. Select *OK* to save the policy.

Installation

The installation tab allows you to view the installation target, device settings status, policy package status, and schedule install status, and edit installation targets for policy package installs. Go to the *Policy & Objects* tab, select the ADOM from the drop-down list, select the policy package in the tree menu, and select the *Installation* tab in the *Policy Package* tab bar.

This page displays the following information:

Installation Target	The installation target and connection status.
Device Settings Status	The device settings synchronization status.
Policy Package Status	The policy package installation status.
Schedule Install	Displays schedule install information.

The following options are available:

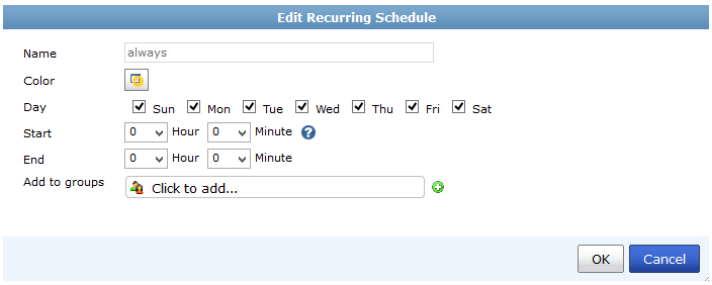
Add	Select to add installation targets (device/group) for the policy package selected. Select the add icon beside *Device/Group* to select devices.
Edit	Select the installation target, right-click, and select *Edit* from the menu.
Delete	Select to delete the selected entries from the installation target for the policy package selected. Delete is also available in the right-click menu.
Install Wizard	Right-click on an entry in the table and select *Install* in the menu to launch the *Install* wizard.
Re-install	Right-click on an entry in the table and select *Re-install* in the menu to perform a quick reinstallation of the policy package to the installation targets.
Add to Schedule	Right-click on an entry in the table and select *Add to Schedule* in the menu to add the item selected to the schedule. This option is only visible when there is an active schedule for the policy package.
Remove from Schedule	Right-click on an entry in the table and select *Remove from Schedule* in the menu to remove the item selected from the schedule. This option is only visible when there is an active schedule for the policy package.
Select All	Right-click on an entry in the table and select *Select ALL* in the menu to select all entries in the table. You can then select to re-install or delete the selected the entries.
Search	Use the search field to search installation targets. Entering text in the search field will highlight matches.

Configuring policy details

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

To edit a policy schedule:

1. Select desired policy tab in the policy toolbar.
2. Select the policy in the table and right-click the *Schedule* column and select *Edit* in the menu. The *Edit Recurring Schedule* dialog box is displayed.



3. Configure the following settings:

Name	Edit the schedule name as required.
Color	Select the icon to select a custom icon to display next to the schedule name.
Day	Select the days of the week for the custom schedule.
Start	Set the schedule start time.
End	Set the schedule end time.
Add to groups	Select to add this policy object to a group.

4. Select *OK* to save the schedule.
   The custom schedule will be added to *Objects* > *Firewall Objects* > *Schedule*.

To edit a policy service:

1. Select desired policy tab in the policy toolbar.
2. Select the policy in the table, right-click the *Service* column, and select *Edit* in the menu. The *Edit Service* dialog box is displayed.
3. Configure the following settings:

Name	Edit the service name as required.
Comments	Type an optional comment.

Color	Select the icon to select an custom icon to display next to the service name.
Protocol	Select the protocol from the drop-down list. Select one of the following: *TCP/UDP/SCTP*, *ICMP*, *ICMP6*, or *IP*.
IP/FQDN	Type the IP address or FQDN. This menu item is available when *Protocol* is set to *TCP/UDP/SCTP*. You can then define the protocol, source port and destination port in the table.
Type	Type the service type in the text field. This menu item is available when *Protocol* is set to *ICMP* or *ICMP6*.
Code	Type the code in the text field. This menu item is available when *Protocol* is set to *ICMP* or *ICMP6*.
Protocol Number	Type the protocol number in the text field. This menu item is available when *Protocol* is set to *IP*.
Advanced Options	For more information on advanced option, see the *FortiOS CLI Reference*.
check-reset-range	Configure ICMP error message verification. • `disable`: The FortiGate unit does not validate ICMP error messages. • `strict`: If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) | TCP(C,D) header, then if FortiManager can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If is enabled the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the `anti-replay` option checks packets. • `default`: Use the global setting defined in `system global`. This field is available when `protocol` is `TCP/UDP/SCTP`. This field is not available if `explicit-proxy` is enabled.
session-ttl	Type the default session timeout in seconds. The valid range is from 300 - 604 800 seconds. Type `0` to use either the `per-policy session-ttl` or `per-VDOM session-ttl`, as applicable. This is available when `protocol` is `TCP/UDP/SCTP`.
tcp-halfclose-timer	Type how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded.The valid range is from 1 to 86400 seconds. Type `0` to use the global setting defined in `system global`. This is available when `protocol` is `TCP/UDP/SCTP`.

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

4. Select *OK* to save the service. The custom service will be added to *Objects* > *Firewall Objects* > *Service*.

To edit a policy action:

1. Select desired policy tab in the policy toolbar.
2. Select the policy in the table, then right-click the *Action* column.
3. Select either *Accept* or *Deny* in the menu.

To edit policy security profiles:

1. Select desired policy tab in the policy toolbar.
2. Select the policy in the table and right-click the *Profile* column.
3. When you select each security profile option in the right-click menu, you can select the profile object.

To edit policy logging:

1. Select desired policy tab in the policy toolbar.
2. Select the policy in the table and right-click the *Log* column.
3. You can select to disable logging, log all security events, or log all session in the menu.

Column options

For many of the policy tabs you can right-click the column header to access the column setting and column filters options. The columns and columns filters available are dependent on the tab and the ADOM firmware version.

Sequence number column options

To change the policy order by sequence number, you can left-click and drag-and-drop the policy.

Right-click in the *Seq.#* column to access the right-click menu. The following options are available:

Create New	Select to create a new policy.
Insert Policy	Select to insert a policy above or below the policy selected.
Edit	Select to edit the selected policy. The *Edit Policy* window opens. Make the required changes then select *OK* to save the changes.
Delete	Select to delete the policy selected. Select *OK* in the confirmation dialog box to continue.
Clone	Select to clone the selected policy. The *Clone Policy* window opens. Make the required changes then select *OK* to save the cloned policy.
Copy	Select to copy the policy selected.
Cut	Select to cut the policy selected.
Paste	Select to paste the selected policy. Select the location where you want to paste the policy then select to paste above or below the policy.
Cancel Copy/Cut	Select to cancel a copy or cut action.
Add Section	Select to add a section above or below the policy selected.
Enable	Select to enable the policy selected.
Disable	Select to disable the policy selected.

Source and destination interface column options

To change the source or destination interface of the policy to match another policy, you can left-click and drag-and-drop the policy object.

Right-click in the *Source Interface* or *Destination Interface* column to access the right-click menu. The following options are available:

Add Object(s)	Select to add source or destination interface objects. The *Add Source Interface* or *Add Destination Interface* dialog box opens. Select objects to add to the policy. Press and hold the control key to add multiple objects. Select *OK* to add the objects.
Remove Object(s)	Select the object then select *Remove Object(s)* to remove the object. Press and hold the control key to remove multiple objects.

Edit	Select to edit the object.
Copy	Select to copy the object.
Cut	Select to cut the object.
Paste	Paste the object that you copied or cut.
Select All	Select all entries in this column entry.

Source and destination column options

To change the source or destination address of the policy to match another policy, you can left-click and drag-and-drop the policy object.

To apply a column filter to this column, right-click the column header and select *Column Filter* from the menu. The *Column Filter* dialog box opens. Select the action, value, and select *Add* to add the filter. Select *Apply* to apply the column filter. You can also select to clear all filters.

Right-click in the *Source* or *Destination* column to access the right-click menu. The following options are available:

Right-click menu options will vary depending on whether you click on the column cell or an object in the column cell.

Add Object(s)	Select to add source or destination address objects. The *Add Source Address or Add Destination Address* dialog box opens. Select objects to add to the policy. Press and hold the control key to add multiple objects. Select *OK* to add the objects.
Remove Object(s)	Select the object and select *Remove Object(s)* to remove the object. Press and hold the control key to remove multiple objects.
Edit	Select to edit the object.
Copy	Select to copy the object.
Cut	Select to cut the object.
Paste	Paste the object you copied or cut.
Negate Cell	Select to negate the cell.
Where Used	Select to check where the object is used. A dialog box will be displayed listing all instances of the object selected.
Select All	Select all entries in this column entry.

Schedule column options

To change the recurring schedule of the policy to match another policy, you can left-click and drag-and-drop the policy object.

To apply a column filter to this column, right-click the column header and select *Column Filter* from the menu. The *Column Filter* dialog box opens. Select the action, value, and select *Add* to add the filter. Select *Apply* to apply the column filter. You can also select to clear all filters.

Right-click in the *Schedule* column to access the right-click menu. The following options are available:

Right-click menu options will vary depending on whether you click on the column cell or an object in the column cell.

Add Object(s)	Select to add schedule objects. The *Add Service* dialog box opens. Select objects to add to the policy. Press and hold the control key to add multiple objects. Select *OK* to add the objects.
Remove Object(s)	Select the object and select *Remove Object(s)* to remove the object. Press and hold the control key to remove multiple objects.
Edit	Select to edit the object. See To edit a policy schedule: on page 274.
Where Used	Select to check where the object is used. A dialog box will be displayed listing all instances of the object selected.

Service column options

To change the service of the policy to match another policy, you can left-click and drag-and-drop the policy object.

To apply a column filter to this column, right-click the column header and select *Column Filter* from the menu. The *Column Filter* dialog box opens. Select the action, value, and select *Add* to add the filter. Select *Apply* to apply the column filter. You can also select to clear all filters.

Right-click in the *Service* column to access the right-click menu. The following options are available:

Right-click menu options will vary depending on whether you click on the column cell or an object in the column cell.

Add Object(s)	Select to add service objects. The *Add Service* dialog box opens. Select objects to add to the policy. Press and hold the control key to add multiple objects. Select *OK* to add the objects.
Remove Object(s)	Select the object and select *Remove Object(s)* to remove the object. Press and hold the control key to remove multiple objects.
Edit	Select to edit the object. See To edit a policy service: on page 274.
Copy	Select to copy the object.

Cut	Select to cut the object.
Paste	Paste the object you copied or cut.
Negate Cell	Select to negate the cell.
Where Used	Select to check where the object is used. A dialog box will be displayed listing all instances of the object selected.
Select All	Select all entries in this column entry.

Authentication column options

To change the authentication user group of the policy to match another policy, you can left-click and drag-and-drop the policy object.

To apply a column filter to this column, right-click the column header and select *Column Filter* from the menu. The *Column Filter* dialog box opens. Select the action, value, and select *Add* to add the filter. Select *Apply* to apply the column filter. You can also select to clear all filters.

Right-click in the *Authentication* column to access the right-click menu. The following options are available:

Right-click menu options will vary depending on whether you click on the column cell or an object in the column cell.

Add Object(s)	Select to add authentication objects. The *Add Authentication* dialog box opens. Select objects to add to the policy. Press and hold the control key to add multiple objects. Select *OK* to add the objects.
Remove Object(s)	Select the object and select *Remove Object(s)* to remove the object. Press and hold the control key to remove multiple objects.
Edit	Select to edit the authentication object selected.
Where Used	Select to check where the object is used. A dialog box will be displayed listing all instances of the object selected.
Select All	Select all entries in this column entry.

Action column options

To apply a column filter to this column, right-click the column header and select *Column Filter* from the menu. The *Column Filter* dialog box opens. Select the action, value, and select *Add* to add the filter. Select *Apply* to apply the column filter. You can also select to clear all filters.

See To edit a policy action: on page 276 for more information.

Right-click in the *Action* column to access the right-click menu. The following options are available:

Accept	Select to set the policy action to accept.
Deny	Select to set the policy action to deny.
IPSEC	There is no right-click menu available when the option is IPSEC.

Profile column options

To change the security profile of the policy to match another policy, you can left-click and drag-and-drop the policy object.

See To edit policy security profiles: on page 276 for more information.

To apply a column filter to this column, right-click the column header and select *Column Filter* from the menu. The *Column Filter* dialog box opens. Select the action, value, and select *Add* to add the filter. Select *Apply* to apply the column filter. You can also select to clear all filters.

Right-click in the *Profile* column to access the right-click menu. The following options are available:

AntiVirus	Enable this option, then select the profile from the second level menu. Select *None* to disable this feature.
Web Filter	Enable this option, then select the profile from the second level menu. Select *None* to disable this feature.
Application Control	Enable this option, then select the profile from the second level menu. Select *None* to disable this feature.
IPS	Enable this option, then select the profile from the second level menu. Select *None* to disable this feature.
Email Filter	Enable this option, then select the profile from the second level menu. Select *None* to disable this feature.
DLP Sensor	Enable this option, then select the profile from the second level menu. Select *None* to disable this feature.
VoIP	Enable this option, then select the profile from the second level menu. Select *None* to disable this feature.
Proxy Option	Enable this option, then select the profile from the second level menu.
SSL/SSH Inspection	Enable this option, then select the profile from the second level menu. Select *None* to disable this feature.

Log column options

To apply a column filter to this column, right-click the column header and select *Column Filter* from the menu. The *Column Filter* dialog box opens. Select the action, value, and select *Add* to add the filter. Select *Apply* to apply the column filter. You can also select to clear all filters.

See To edit a policy schedule: on page 274 for more information.

Right-click in the *Log* column to access the right-click menu. The following options are available:

Disable	Select to disable logging.
Log Security Events	Select to log security events only.
Log All Sessions	Select to log all sessions.

NAT column options

To apply a column filter to this column, right-click the column header and select *Column Filter* from the menu. The *Column Filter* dialog box opens. Select the action, value, and select *Add* to add the filter. Select *Apply* to apply the column filter. You can also select to clear all filters.

Right-click in the *NAT* column to access the right-click menu. The following options are available:

Disable	Select to disable NAT.
Use Destination Address	Select to use destination address.
Dynamic IP Pool	Select to use dynamic IP pool, if configured.

Install On column options

To apply a column filter to this column, right-click the column header and select *Column Filter* from the menu. The *Column Filter* dialog box opens. Select the action, value, and select *Add* to add the filter. Select *Apply* to apply the column filter. You can also select to clear all filters.

Right-click in the *Install On* column to access the right-click menu. The following options are available:

Right-click menu options will vary depending on whether you click on the column cell or an object in the column cell.

Add Object(s)	Select to change the install on value. The Add Install dialog box is displayed. Select objects then select *OK*.
Remove Object(s)	Select to remove an install on entry.
Set To Default	Select to set to the default value.
Where Used	Select to check where the object is used. A dialog box will be displayed listing all instances of the object selected.
Select All	Select to select all entries in this column entry.

Section right-click menu options

After you have created a new section, you can right-click the section to access the section right-click menu. The following options are available:

Append Policy	Select to append the policy to the section selected.
Edit Title	Select to edit the section title.
Delete	Select to delete the section selected.
Collapse All	Select to collapse all policies under the section selected.
Expand All	Select to expand all policies under the section selected.

	The *ID*, *Tags*, and *Comments* columns do not have a right-click menu.

	Left-click in a comments column cell to add or edit the policy comments. The comments field character limit is 1023 characters.

	Left-click a tag in the *Tags* column to delete the tag. Select *OK* in the confirmation dialog box.

UUID column right-click menu options

To apply a column filter to this column, right-click the column header and select *Column Filter* from the menu. The *Column Filter* dialog box opens. Select the action, value, and select *Add* to add the filter. Select *Apply* to apply the column filter. You can also select to clear all filters.

Right-click in the *UUID* column to access the right-click menu. The following options are available:

Copy UUID	Select to copy the UUID to the clipboard.
View Log	Select to view the log by UUID.

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 *Tools* > *ADOM Revisions* menu option in the *Policy & Objects* tab.

This page displays the following:

ID	The ADOM revision identifier.

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

The following options are available:

Edit	Right-click on a revision in the table and select *Edit* in the menu to edit the ADOM revision.
Delete	Right-click on a revision in the table and select *Delete* in the menu to delete the ADOM revision. When *Lock this revision from auto deletion* is selected, you are not able to delete the ADOM revision.
Restore	Right-click on a revision in the table and select *Restore* in the menu to restore the ADOM revision. Restoring a revision will revert policy packages, objects and VPN console to the selected version. Select *OK* to continue.
Lock	Right-click on a revision in the table and select *Lock* in the menu to lock this revision from auto deletion.
Unlock	Right-click on a revision in the table and select *Unlock* in the menu to unlock this revision. When the ADOM revision is in an unlocked state, auto deletion will occur in accordance with your auto deletion settings.
View Revision Diff	Right-click on a revision in the table and select *View Revision Diff* in the menu. The Summary page will be displayed. This page shows the revision differences between the selected revision and the current database.
Select All	Right-click on a revision in the table and select *Select All* in the menu. You can then select to *Delete* all unlocked ADOM revisions.
Create New	Select to create a new ADOM revision.
Close	Select to close the *ADOM Revision* dialog box and return to the *Policy & Objects* tab.

To create a new ADOM revision:

1. Go to the *Policy & Objects* tab and select *Tools > ADOM Revisions* in the toolbar. The *ADOM Revisions* window opens.
2. Select *Create New*. The *Create New ADOM Revision* dialog box opens.

3. Type a name for the revisions in the *Name* field.
4. Optionally, type a description of the revision in the *Description* field.
5. To prevent the revision from being automatically deleted, select *Lock this revision from auto deletion*.
6. To configure the automatic deletion of revisions, select *[Details]*.
7. Select *OK* to create the new ADOM revision.

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 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 menu.
3. To delete multiple revisions, use the Control or Shift keys on your keyboard to select multiple revisions, or right-click on a revision and select *Select All* from the menu to select all of the revision. Then, right-click on any one of the selected revisions and select *Delete* from the menu.
4. Select *OK* in the confirmation dialog box to delete the selected revision or revisions.

To configure automatic deletion:

1. Open the *ADOM Revisions* window.
2. Right-click on any revision in the table and select *Edit* from the menu.
3. In the *Edit ADOM Revision* dialog box select *[Details]*. The *Configuration* dialog box opens.
4. To enable to automatic deletion of revisions, select *Auto Delete Revisions*.
5. Select one of the two available options for automatic deletion of revisions:
6. *Keep last x Revisions*: Only keep the entered numbered of revisions, deleting the oldest revision when a new revision is created.
7. *Delete revision older than x Days*: Delete all revisions that are older than the entered number of days.
8. Select *OK* to apply the changes, then select *OK* again in the *Edit ADOM Revision* dialog box.

To restore a previous ADOM revision:

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

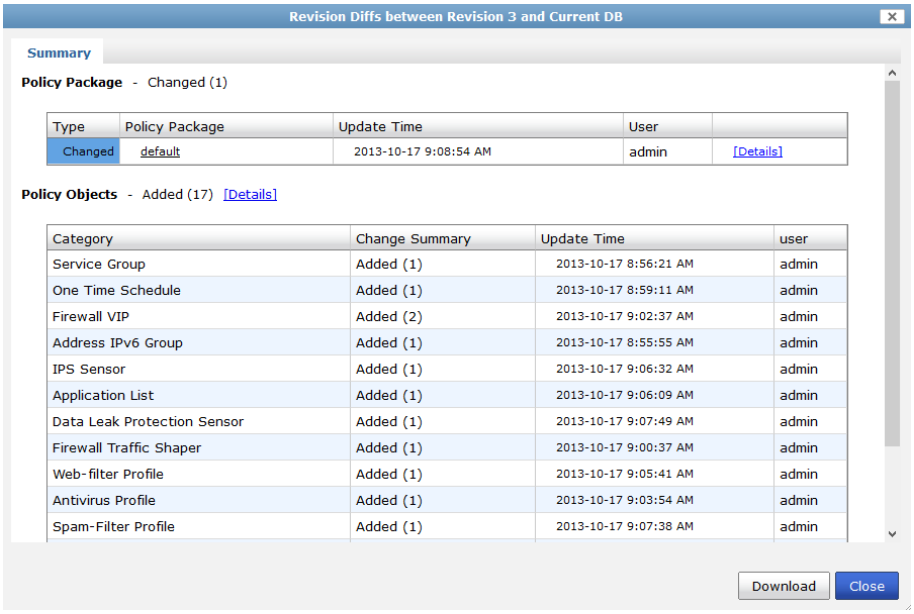
To lock or unlock an ADOM revision:

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 menu.
- Edit the revision and select or deselect *Lock this revision from auto deletion* from the *Edit ADOM Revision* dialog box.

To view ADOM revision diff:

1. Open the *ADOM Revisions* window.
2. Right-click on a revision in the table and select *View Revision Diff* from the menu. The *Summary* page will load.



This page displays all *Policy Package* and *Policy Object* changes between the revision selected and the current database.

3. Select *[Details]* to view all details on the changes made to policies and objects.
4. You can select to download this information as a CSV file to your management computer.
5. Select *Close* to return to the *Policy & Objects* page.

Managing objects and dynamic objects

All objects within an ADOM are managed by a single database unique to that ADOM. Objects inside that database can include items such as addresses, services, intrusion protection definitions, antivirus signatures, web filtering profiles, etc.

Many objects now include the option to enable dynamic mapping. You can create new dynamic maps. When this feature is enabled, a table is displayed which lists the dynamic mapping information. You can also select to add the object to groups, when available, and add tags.

When making changes to an object within the object database, changes are reflected immediately within the policy table in the GUI; no copying to the database is required.

Dynamic objects are used to map a single logical object to a unique definition per device. Addresses, interfaces, virtual IPs, and an IP pool can all be addressed dynamically.

Not all policy and object options are enabled by default. See Display options on page 252.

Objects and dynamic objects are managed in lower frame of the *Policy & Objects* tab. The available objects varies depending on the specific ADOM selected.

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 293.

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.

Right-click on an object to find out where the object is used (*Where Used*) or to add the object to a group (*Grouping*).

FortiManager objects are defined either per ADOM or at a global level. In the *Policy & Objects* tab, either select the ADOM from the drop-down list or select Global. Objects are displayed in the content pane.

Objects Type	Available Objects	Level
Interface	• Interface • Zone • Create a new interface or zone • Dynamic Mapping option	ADOM and Global

Objects Type	Available Objects	Level
Firewall Objects	• Address Create a new Address, Address Group, IPv6 Address, or IPv6 Address Group. You can select to add the object to groups and enable dynamic mapping. When enabling dynamic mapping, select *Create New* to edit the mapped device, and map to address. • Service Create a new Service (Firewall or Explicit Proxy) or Service Group. You can select to add the object to groups. • Schedule Create a new Recurring Schedule, One-time Schedule, or Schedule Group. You can select to add the object to groups. • Traffic Shaper Create a new Shared Shaper or Per-IP Shaper. • Virtual IP Create a new IPv4 Virtual IP, IPv6 Virtual IP, NAT64 Virtual IP, NAT46 Virtual IP, IPv4 VIP Group, IPv6 VIP Group, NAT64 VIP Group, NAT 46 VIP Group, IP Pool, or IPv6 IP Pool. You can select to add the object to groups and enable dynamic mapping. When enabling dynamic mapping, select *Create New* to edit the mapped device, and map to address. • Load Balance • Virtual Server • Real Server • Health Check Monitor • Web Proxy Forwarding Server Create a new Web Proxy Forwarding Server.	ADOM and Global Load Balance is available at the ADOM level only.

Objects Type	Available Objects	Level
Security Profiles	• AntiVirus Profile • Web Filter Profile • Application Sensor • IPS Sensor • Email Filter Profile • Data Leak Prevention Sensor • VoIP Profile • ICAP Profile • MMS Profile Create a new MMS Profile. (FortiCarrier only) • GTP Profile Create a new GTP Profile. (FortiCarrier only) • Advanced • Application List Create a Custom Application Signature. • Web Content Filter • Web URL Filter • Local Category • Rating Overrides Create a New Local Rating. • IPS Custom Signature Create a New Custom Signature. • Email List • File Filter • Detection List • ICAP Server Create a New ICAP Server. • Proxy Options Create new Proxy Options. • SSL/SSH Inspection • Create New Deep Inspection Options. • Profile Group Create a new Profile Group. • SSL VPN Portal Create a new SSL VPN Portal.	ADOM and Global

Objects Type	Available Objects	Level
User & Device	• User Definition Create a New User. You can select to add the object to groups. • POP3 User Create a new POP3 user. • User Group Create a New User Group. Add remote authentication servers. • Device Create a new Device or Device Group. • Remote Create a new LDAP, RADIUS, or TACACS+ Server. Dynamic Mapping option. • PKI Create a New PKI User. • SMS Service Create a new SMS Server. • FortiToken Add a new FortiToken. • Single Sign-On Create a New RADIUS Single Sign-On Agent and Retrieve FSSO Agent.	ADOM and Global
WAN Opt	• Profile Create a new WAN Optimization Profile. • Peer Create a new WAN Optimization Peer. • Authentication Group Create a new Authentication Group.	ADOM and Global
Dynamic Objects	• Local Certificate Create a New Dynamic Local Certificate. • VPN Tunnel Create a New Dynamic VPN Tunnel. You can select to enable dynamic mapping. When enabling dynamic mapping, select *Create New* to edit the mapped device and VPN tunnel.	ADOM only

Objects Type	Available Objects	Level
CLI-Only Objects	Configure CLI only objects. The available objects are dependent on the ADOM version and device options.	ADOM and Global
Advanced	• Replacement Message Group Create a new replacement message group.	ADOM and Global
Advanced	• CA Certificate Import and view CA Certificates.	ADOM only
Advanced	• Tag Management Create a new Tag.	ADOM and Global
Advanced	• Script Create or import a new script.	Global only

Lock an ADOM

If workspace is enabled, you must lock an ADOM prior to performing any management tasks on it. See Lock an ADOM or policy package on page 252 for instructions.

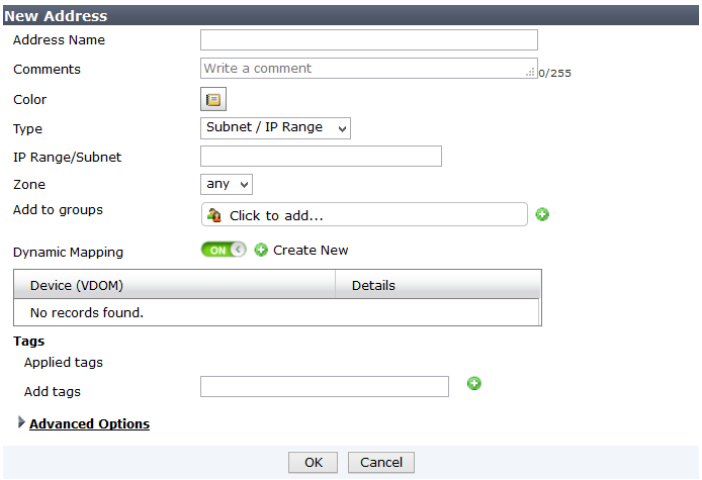
Create a new object

Objects can be created as global objects, or for specific ADOMs.

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 content pane. The available address or address group lists are selectable on the 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. The *New Address* dialog window will open.



In v5.2.0 or later, you can select to add the object to groups and enable dynamic mapping. These options are not available for all objects.

4. Enter the required information, depending on the object selected, and then select *OK* to create the new object.

Map a dynamic object

The devices and VDOMs to which a global object is mapped can also be viewed from the object list. In v5.2 or later, you can add an object to groups and enable dynamic mapping. These options are not available for all objects.

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

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 menu.

Edit an object

After editing an object in the object database, the changes are immediately reflected within the policy table in the GUI; no copying to the database is required.

To edit an object:

1. 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 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 menu. The *Edit* dialog box opens.
3. Adjust the information as required, and then select *OK* to create the new object.
4. Browse to the location of the object in the object tree menu or policy.
5. Right-click on the object or group and select *Where Used* from the menu.

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 type a search keyword. The results of the search are updated as you type and displayed in the object list.

Drag and drop objects

Objects can be dragged and dropped from the object frame, or from other policies, 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.

CLI-Only objects

FortiManager v5.2.0 or later adds the ability to configure objects in the GUI which are available only configurable via the FortiOS command line interface.

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. Type 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* > *User Definition* to create a new user.

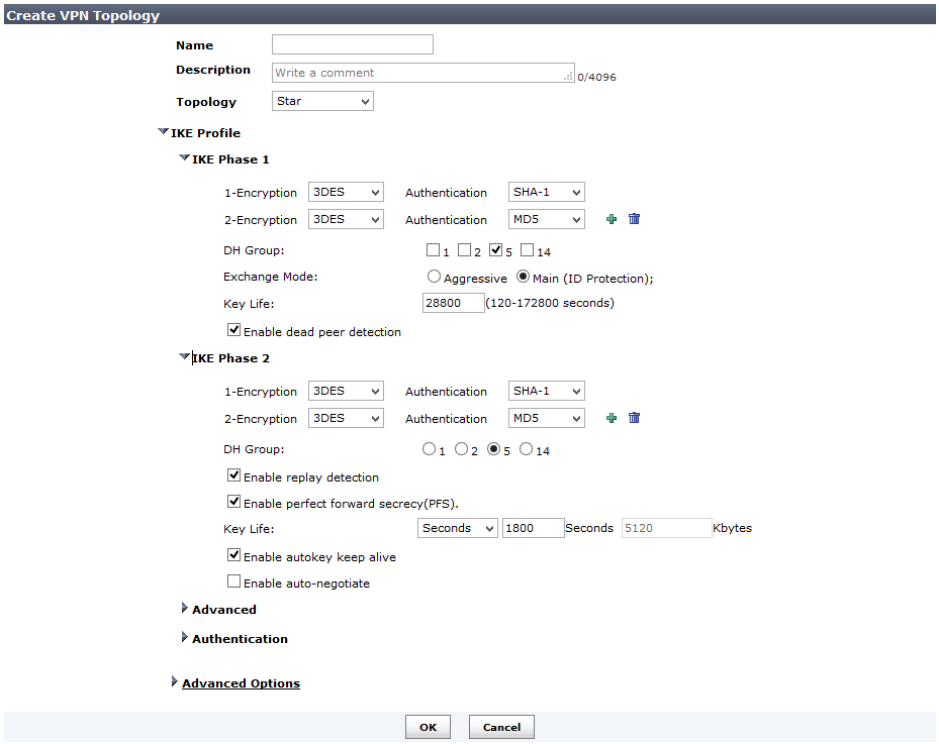
5. When creating the new user, select *Enable Two-factor Authentication,* and then select the FortiToken from the drop down menu.
6. Browse to *User & Device* > *User Group*, create a new user group, and add the previously created user to this group.
7. Install a policy package to the FortiGate, as described in Install a policy package on page 255..
8. On the FortiGate, select *User* > *FortiToken*. Select one of the newly created FortiTokens, then select *OK* to activate the FortiToken unit.

Central VPN Console

When Central VPN Console is selected for VPN Management when creating an ADOM, a VPN Console tree menu item will appear in the *Policy & Objects* tab under Policy Package. You will need to enable the *Show VPN Console* option in *System Settings* > *Admin* > *Admin Settings*. You can create VPN topologies in this page. Once you have configured a VPN topology and gateway, you can configure the related firewall policies, preview and install. For more information, see Managing policies on page 257.

VPN topology

You can create full meshed, star, and dial up VPN topologies. Once you have created the topology, you can create the VPN gateway.



Configure the following settings:

Name	Type a name for the VPN topology.
Description	Type an optional description.

Topology	Select the topology type from the drop-down list. Select one of: • *Full Meshed*: Each gateway has a tunnel to every other gateway. • *Star*: Each gateway has one tunnel to a central hub gateway. • *Dial up*: Some gateways, often mobile users, have dynamic IP addresses and contact the gateway to establish a tunnel.
IKE Profile	Define the IKE Profile. Configure IKE Phase 1, IKE Phase 2, Advanced settings, and Authentication settings.
IKE Phase 1	Define the IKE Phase 1 proposal settings .
Encryption Authentication	Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of three combinations. The remote peer or client must be configured to use at least one of the proposals that you define. Select one of the following symmetric-key encryption algorithms: • DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • 3DES: Triple-DES, in which plain text is encrypted three times by three keys. • AES128: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key. • AES192: A128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key. • AES256: A128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key. Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations: • MD5: Message Digest 5, the hash algorithm developed by RSA Data Security. • SHA1: Secure Hash Algorithm 1, which produces a 160-bit message digest. • SHA256: Secure Hash Algorithm 2, which produces a 256-bit message digest. To specify a third combination, use the Add button beside the fields for the second combination.
DH Group	Select one or more Diffie-Hellman groups from DH group 1, 2, 5 and 14. At least one of the DH Group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations. Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.

	Exchange Mode	Select either *Aggressive* or *Main (ID Protection)*. The FortiGate unit and the remote peer or dialup client exchange phase 1 parameters in either Main mode or Aggressive mode. This choice does not apply if you use IKE version 2, which is available only for route-based configurations. • In Main mode, the Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information • In Aggressive mode, the Phase 1 parameters are exchanged in single message with authentication information that is not encrypted. Although Main mode is more secure, you must select Aggressive mode if there is more than one dialup Phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier local ID). Descriptions of the peer options in this guide indicate whether Main or Aggressive mode is required.
	Key Life	Type the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The keylife can be from 120 to 172800 seconds.
	Enable dead peer detection	Select this check box to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required. You can use this option to receive notification whenever a tunnel goes up or down, or to keep the tunnel connection open when no traffic is being generated inside the tunnel. For example, in scenarios where a dialup client or dynamic DNS peer connects from an IP address that changes periodically, traffic may be suspended while the IP address changes.
IKE Phase 2		Define the IKE Phase 2 proposal settings. When you define phase 2 parameters, you can choose any set of phase 1 parameters to set up a secure connection for the tunnel and authenticate the remote peer. Auto Key configuration applies to both tunnel-mode and interface-mode VPNs.

	Encryption Authentication	Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of three combinations. The remote peer or client must be configured to use at least one of the proposals that you define. It is invalid to set both Encryption and Authentication to NULL. Select one of the following symmetric-key encryption algorithms: • NULL: Do not use an encryption algorithm. • DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • 3DES: Triple-DES, in which plain text is encrypted three times by three keys. • AES128: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key. • AES192: A128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key. • AES256: A128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key. Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations: • NULL: Do not use a message digest. • MD5: Message Digest 5, the hash algorithm developed by RSA Data Security. • SHA1: Secure Hash Algorithm 1, which produces a 160-bit message digest. • SHA256: Secure Hash Algorithm 2, which produces a 256-bit message digest. To specify a third combination, use the Add button beside the fields for the second combination.
	DH Group	Select one or more Diffie-Hellman groups from DH group 1, 2, 5 and 14. At least one of the DH Group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations. Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.
	Enable replay detection	Select to enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.
	Enable perfect forward secrecy (PFS)	Select to enable or disable perfect forward secrecy (PFS). Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.

	Key Life	Select the PFS key life. Select *Second, Kbytes,* or *Both* from the drop-down list and type the value in the text field.
	Enable autokey keep alive	Select to enable or disable autokey keep alive. The phase 2 SA has a fixed duration. If there is traffic on the VPN as the SA nears expiry, a new SA is negotiated and the VPN switches to the new SA without interruption. If there is no traffic, the SA expires and the VPN tunnel goes down. A new SA will not be generated until there is traffic. The Autokey Keep Alive option ensures that a new SA is negotiated even if there is no traffic so that the VPN tunnel stays up.
	Enable auto-negotiate	Select to enable or disable auto-negotiation.
Advanced		
	Enable NAT Traversal	Select the check box if a NAT device exists between the local FortiGate unit and the VPN peer or client. The local FortiGate unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared) to connect reliably.
	NAT Traversal Keep-alive Frequency	If you enabled NAT-traversal, type a keep-alive frequency setting (10-900 seconds).
Authentication		The FortiGate unit implements the Encapsulated Security Payload (ESP) protocol. Internet Key Exchange (IKE) is performed automatically based on pre-shared keys or X.509 digital certificates. As an option, you can specify manual keys. Interface mode, supported in NAT mode only, creates a virtual interface for the local end of a VPN tunnel.
	Pre-shared Key	If you selected Pre-shared Key, type the pre-shared key that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. You must define the same key at the remote peer or client. The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters. Alternatively, you can select to generate a random pre-shared key.
	Certificates	If you selected Certificates, select the name of the server certificate that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. For information about obtaining and loading the required server certificate, see the *FortiOS User Authentication* guide.
Advanced-Options		For more information on advanced option, see the *FortiOS 5.2 CLI Reference*.

fcc-enforcement	Select to enable or disable FCC enforcement.
ike-version	Select the version of IKE to use. This is available only if IPsec Interface Mode is enabled. For more information about IKE v2, refer to RFC 4306. IKE v2 is not available if *Exchange Mode* is *Aggressive*. When IKE Version is set to 2, Mode and XAUTH are not available.
inter-vdom	Select to enable or disable the inter-vdom setting.
loccalid-type	Select the local ID type from the drop-down list. Select one of: • auto: Select type automatically • fqdn: Fully Qualified Domain name • user-fqdn: User Fully Qualified Domain Name • keyid: Key Identifier ID • address: IP Address • asn1dn: ASN.1 Distinguished Name
negotiate-timeout	Type the negotiation timeout value. The default is 30 seconds.

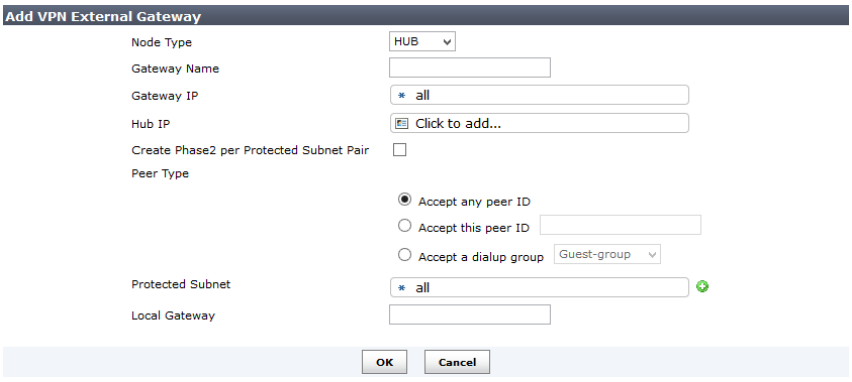
Once you have created your VPN topology, you can select to create a new managed gateway or external gateway for the topology.

VPN gateway

Once you have created the VPN topology, you can create a managed or external gateway. The settings on these pages are dependent on the VPN topology selected.

Create a VPN external gateway:

1. Select the VPN topology, right-click, and select *Config Gateways* in the menu.
2. Select *Create New* in the toolbar and select to create an *External Gateway*. The *Add VPN External Gateway* page opens.



3. Configure the following settings:

Node Type	Select either *HUB* or *Spoke* from the drop-down list. This menu item is available when *Topology* is *Star* or *Dial up*.
Gateway Name	Type the gateway name.
Gateway IP	Select the gateway IP address from the drop-down list.
Hub IP	Select the hub IP address from the drop-down list. This menu item is available when *Topology* is *Star* or *Dial up* and *Node Type* is *HUB*.
Create Phase2 per Protected Subnet Pair	Select the checkbox to create a phase2 per protected subnet pair.
Peer Type	Select the peer type. Select one of the following: • Accept any peer ID • Accept this peer ID (type the peer ID in the text field) • Accept a dialup group (select the group from the drop-down list) A Local ID is an alphanumeric value assigned in the Phase 1 configuration. The Local ID of a peer is called a Peer ID. The Local ID or peer ID can be used to uniquely identify one end of a VPN tunnel. This enables a more secure connection. Also if you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect. When you configure it on your end, it is your Local ID. When the remote end connects to you, they see it as your peer ID. If you are debugging a VPN connection, the Local ID is part of the VPN negotiations. You can use it to help troubleshoot connection problems. The default configuration is to accept all local IDs (peer IDs). If you have the Local ID set, the remote end of the tunnel must be configured to accept your Local ID. This menu item is available when *Topology* is *Dial up*.
Protected Subnet	Select the address or address group from the drop-down list and select the add icon to add the entry. You can add multiple entries.
Local Gateway	Type the local gateway IP address in the text field.

4. Select *OK* to save the settings.
5. Select *Return* to return to the VPN topology page.

Create a VPN managed gateway:

1. Select the VPN topology, right-click, and select *Config Gateways* in the menu.
2. Select *Create New* in the toolbar and select to create a *Managed Gateway*. The *Add VPN Managed Gateway* page opens.
3. Configure the following settings:

Node Type	Select either *HUB* or *Spoke* from the drop-down list. This menu item is available when *Topology* is *Star* or *Dial up*.

Device	Select the device from the drop-down list.
Default VPN Interface	Select the default VPN interface from the drop-down list.
Hub-to-Hub Interface	Select the hub-to-hub interface from the drop-down list. This field is mandatory for multiple hubs. This menu item is available when *Topology* is *Star* or *Dial up* and *Node Type* is *HUB*.
Peer Type	Select the peer type. Select one of the following: • Accept any peer ID • Accept this peer ID (type the peer ID in the text field) • Accept a dialup group (select the group from the drop-down list) This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
Routing	Select either *Manual (via Device Manager)* or *Automatic*.
Summary Network(s)	Select the address or address group from the drop-down list, select the priority and select the add icon to add the entry. You can add multiple entries. This menu item is available when *Topology* is *Star* or *Dial up* and *Node Type* is *HUB*.
Protected Subnet	Select the address or address group from the drop-down list and select the add icon icon to add the entry. You can add multiple entries.
Enable IKE Configuration Method (“mode config”)	Select to enable *IKE Configuration Method*. This menu item is available when *Topology* is *Dial up*.
Enable IP Assignment	Select to enable IP assignment. This menu item is available when *Topology* is *Dial up*.
IP Assignment Mode	Select either *Range* or *User Group* from the drop-down list. This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
IP Assignment Type	Select either *IP* or *Subnet* from the drop-down list. This menu item is available when *Topology* is *Dial up*, *Node Type* is *HUB*, and *IP Assignment Mode* is *Range*.
IPv4 Start IP	Type the IPv4 start IP address. This menu item is available when *Topology* is *Dial up*, *Node Type* is *HUB*, and *IP Assignment Mode* is *Range*.
IPv4 End IP	Type the IPv4 end IP address. This menu item is available when *Topology* is *Dial up*, *Node Type* is *HUB*, and *IP Assignment Mode* is *Range*.
IPv4 Netmask	Type the IPv4 network mask. This menu item is available when *Topology* is *Dial up*, *Node Type* is *HUB*, and *IP Assignment Mode* is *Range*.

Add Route	Select the checkbox to add a route for this entry. This menu item is available when *Topology* is *Dial up*.
DNS Server #1	Type the DNS server IP address to provide IKE Configuration Method to clients. This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
DNS Server #2	Type the DNS server IP address to provide IKE Configuration Method to clients. This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
DNS Server #3	Type the DNS server IP address to provide IKE Configuration Method to clients. This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
WINS Server #1	Type the WINS server IP address to provide IKE Configuration Method to clients. This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
WINS Server #2	Type the WINS server IP address to provide IKE Configuration Method to clients. This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
IPv4 Split Include	Select the address or address group from the drop-down list. This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
Local Gateway	Type the local gateway IP address in the text field.
Exclusive IP Range	Type the start IP and end IP and select the add icon to add the entry. You can add multiple entries. This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
Advanced Options	For more information on advanced options, see the *FortiOS 5.2 CLI Reference*.
authpasswd	Type the XAuth client password for the FortiGate. This field is available when `xauthtype` is set to client.
authusr	Type the XAuth client user name for the FortiGate. This field is available when `xauthtype` is set to client.

authusrgrp	Select the authentication user group from the drop-down list. This field is available when xauthtype is set to auto, pap, or chap. When the FortiGate unit is configured as an XAuth server, type the user group to authenticate remote VPN peers. The user group can contain local users, LDAP servers, and RADIUS servers. The user group must be added to the FortiGate configuration before the group name can be cross referenced.
banner	Type the banner value. Specify a message to send to IKE Configuration Method clients. Some clients display this message to users. This is available if mode-cfg (IKE Configuration Method) is enabled.
dns-mode	Select either manual or auto from the drop-down list. • auto: Assign DNS servers in the following order: • Servers assigned to interface by DHCP. • Per-VDOM assigned DNS servers. • Global DNS servers. • manual: Use DNS servers specified in DNS Server 1, DNS Server 2 etc.
domain	Type the domain value.
public-ip	Type the public IP address value. Use this field to configure a VPN with dynamic interfaces. Define a `public-ip` value here, which is the dynamically assigned PPPoE address, which remains static and does not change over time.
unity-support	Select either enable or disable from the drop-down list.
xauthtype	Select the XAuth type from the drop-down list. Select one of: disable, client, pap, chap, or auto.

4. Select *OK* to save the settings.
5. Select *Return* to return to the VPN topology page.

VPN security policies

Once you have defined the IP source and destination addresses, the phase 1 authentication parameters, and the phase 2 parameters, you must define the VPN security policies.

FortiGate unit VPNs can be policy-based or route-based. There is little difference between the two types. In both cases, you specify phase 1 and phase 2 settings. However there is a difference in implementation. A route-based VPN creates a virtual IPsec network interface that applies encryption or decryption as needed to any traffic that it carries. That is why route-based VPNs are also known as interface-based VPNs. A policy-based VPN is implemented through a special security policy that applies the encryption you specified in the phase 1 and phase 2 settings.

An IPsec security policy enables the transmission and reception of encrypted packets, specifies the permitted direction of VPN traffic, and selects the VPN tunnel. In most cases, a single policy is needed to control both inbound and outbound IP traffic through a VPN tunnel.

For a route-based VPN, you create two security policies between the virtual IPsec interface and the interface that connects to the private network. In one policy the virtual interface is the source. In the other policy the virtual interface is the destination. The Action for both policies is Accept. This creates bidirectional policies that ensure traffic will flow in both directions over the VPN.

For a policy-based VPN, one security policy enables communication in both directions. You must select IPSEC as the Action and then select the VPN tunnel you defined in the phase 1 settings. You can then enable inbound and outbound traffic as needed within that policy, or create multiple policies of this type to handle different types of traffic differently. For example HTTPS traffic may not require the same level of scanning as FTP traffic.

Defining policy addresses

A VPN tunnel has two end points. These end points may be VPN peers such as two FortiGate gateways. Encrypted packets are transmitted between the end points. At each end of the VPN tunnel, a VPN peer intercepts encrypted packets, decrypts the packets, and forwards the decrypted IP packets to the intended destination.

You need to define firewall addresses for the private networks behind each peer. You will use these addresses as the source or destination address depending on the security policy.

In general:

- In a gateway-to-gateway, hub-and-spoke, dynamic DNS, redundant-tunnel, or transparent configuration, you need to define a policy address for the private IP address of the network behind the remote VPN peer.
- In a peer-to-peer configuration, you need to define a policy address for the private IP address of a server or host behind the remote VPN peer.

Defining security policies

Security policies allow IP traffic to pass between interfaces on a FortiGate unit. You can limit communication to particular traffic by specifying source address and destination addresses. Then only traffic from those addresses will be allowed.

Policy-based and route-based VPNs require different security policies.

A policy-based VPN requires an IPsec security policy. You specify the interface to the private network, the interface to the remote peer and the VPN tunnel. A single policy can enable traffic inbound, outbound, or in both directions.

A route-based VPN requires an Accept security policy for each direction. As source and destination interfaces, you specify the interface to the private network and the virtual IPsec interface of the VPN. The IPsec interface is the destination interface for the outbound policy and the source interface for the inbound policy. One security policy must be configured for each direction of each VPN interface.

If the security policy, which grants the VPN connection is limited to certain services, DHCP must be included, otherwise the client will not be able to retrieve a lease from the FortiGate's (IPsec) DHCP server, because the DHCP request (coming out of the tunnel) will be blocked.

Before you define the IPsec policy, you must:

- Define the IP source and destination addresses.
- Specify the phase 1 authentication parameters.
- Specify the phase 2 parameters.

You must define at least one IPsec policy for each VPN tunnel. If the same remote server or client requires access to more than one network behind a local FortiGate unit, the FortiGate unit must be configured with an IPsec policy for each network. Multiple policies may be required to configure redundant connections to a remote destination or control access to different services at different times.

To ensure a secure connection, the FortiGate unit must evaluate IPSEC policies before ACCEPT and DENY security policies. Because the FortiGate unit reads policies starting at the top of the list, you must move all IPsec policies to the top of the list. When you define multiple IPsec policies for the same tunnel, you must reorder the IPsec policies that apply to the tunnel so that specific constraints can be evaluated before general constraints.

When you define a route-based VPN, you create a virtual IPsec interface on the physical interface that connects to the remote peer. You create ordinary Accept security policies to enable traffic between the IPsec interface and the interface that connects to the private network. This makes configuration simpler than for policy-based VPNs, which require IPsec security policies.

For more information on IPsec VPN, see the *IPsec VPN for FortiOS* chapter of the *FortiOS Handbook available* from the Fortinet Document Library. See Managing policies on page 257 for information on creating a VPN policy on your FortiManager.

FortiGuard Management

The FortiGuard Distribution Network (FDN) provides FortiGuard services for your FortiManager system and its managed devices and FortiClient agents. The FDN is a world-wide network of FortiGuard Distribution Servers (FDS) which update the FortiGuard services on your FortiManager system on a regular basis so that your FortiManager system is protected against the latest threats.

The FortiGuard services available on the FortiManager system include:

- Antivirus and IPS engines and signatures
- Web filtering and email filtering rating databases and lookups (select systems)
- Vulnerability scan and management support for FortiAnalyzer

To view and configure these services, go to *FortiGuard* > *FortiGuard Management* > *Advanced Settings*.

In FortiGuard Management, you can configure the FortiManager system to act as a local FDS, or use a web proxy server to connect to the FDN. FortiManager systems acting as a local FDS synchronize their FortiGuard service update packages with the FDN, then provide FortiGuard these updates and look up replies to your private network's FortiGate devices. The local FDS provides a faster connection, reducing Internet connection load and the time required to apply frequent updates, such as antivirus signatures, to many devices.

As an example, you might enable FortiGuard services to FortiGate devices on the built-in FDS, then specify the FortiManager system's IP address as the override server on your devices. Instead of burdening your Internet connection with all the devices downloading antivirus updates separately, the FortiManager system would use the Internet connection once to download the FortiGate antivirus package update, then redistribute the package to the devices.

FortiGuard Management also includes firmware revision management. To view and configure firmware options, go to *FortiGuard Management* > *Firmware Images*. You can download these images from the Customer Service & Support portal to install on your managed devices or on the FortiManager system.

Before you can use your FortiManager system as a local FDS, you must:

- Register your devices with Fortinet Customer Service & Support and enable the FortiGuard service licenses. See your device documentation for more information on registering your products.
- If the FortiManager system's Unregistered Device Options do not allow service to unregistered devices, add your devices to the device list, or change the option to allow service to unregistered devices. For more information, see the *FortiManager CLI Reference*.

  For information about FDN service connection attempt handling or adding devices, see Device Manager on page 128.
- Enable and configure the FortiManager system's built-in FDS. For more information, see Configuring network interfaces on page 69.
- 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 313.
- 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 143.

This section contains the following topics:

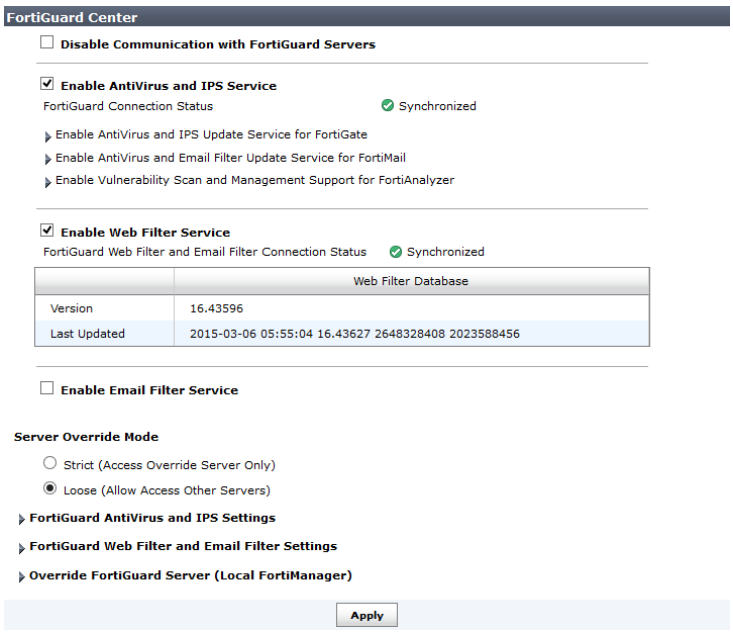
For information on current security threats, virus and spam sample submission, and FortiGuard service updates available through the FDN, including antivirus, IPS, web filtering, and email filtering, see the FortiGuard Center website, http://www.-fortiguard.com/.

Advanced settings

The advanced settings provides a central location for configuring and enabling your FortiManager system's built-in FDS as an FDN override server.

By default, this option is 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. FortiGuard Management 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



Configure the following settings:

Disable communication with the FortiGuard servers.	When disabled, you must upoad packages, databasess, and licenses to your FortiManager.
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: Appears when the FDN connection fails. • Connected: Appears when the initial FDN connection succeeds, but a synchronization connection has not yet occurred. • Out of Sync: Appears when the initial FDN connection succeeds, but the built-in FDS is disabled. • Synchronized: 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. You can select to download updates for FortiOS versions 5.0 (5.2, 5.0,), 4.0 (4.3, 4.2, 4.1, 4.0), and 3.0 (MR7, MR6).
Enable Antivirus and Email Filter Update Service for FortiMail	Select the OS versions from the table for updating antivirus and email filter for FortiMail. You can select to download updates for FortiMail OS versions 5.0 (5.1, 5.0), 4.0 (4.1, 4.0), and 3.0 (MR5, MR4).
Enable Vulnerability Scan and Management Support for FortiAnalyzer	Select the OS versions from the table for supporting Vulnerability Scan and Management Support for FortiAnalyzer. You can select to download updates for FortiAnalyzer OS versions 5.0 (5.0) and 4.0 (4.3, 4.2, 4.1, 4.0).
Enable Web Filter and Services	Select to enable web filter services.
FortiGuard Web Filter and Email Filter Connection Status	The status of the current connection between the FDN and the FortiManager system. See FortiGuard Connection Status on page 309 for more information.
Enable Email Filter Services	Select to enable email filter services.
FortiGuard Web Filter and Email Filter Connection Status	The status of the current connection between the FDN and the FortiManager system. See FortiGuard Connection Status on page 309 for more information.
Server Override Mode	Select *Strict (Access Override Server Only)* or Loose (Allow Access Other Servers) override mode.

FortiGuard Antivirus and IPS Settings	Configure antivirus and IPS settings. See FortiGuard antivirus and IPS settings on page 311.
FortiGuard Web Filter and Email Filter Settings	Configure web and email filter settings. See FortiGuard web and email filter settings on page 311
Override FortiGuard Server (Local FortiManager)	Configure web and email filter settings. See Override FortiGuard server (Local FortiManager) on page 313

When selecting to disable communication with FortiGuard servers, you must manually upload packages for FortiGate, FortiMail, and FortiClient.

The following options are available:

Disable Communication with FortiGuard Servers	Select to disable communication with the FortiGuard servers. When this option is selected, you must manually upload packages for FortiGate, FortiMail, and FortiClient.
Enable Antivirus and IPS Service	Select to enable antivirus and intrusion protection service. When uploaded to FortiManager, the Antivirus and IPS database is displayed.
Enable Web Filter Services	Select to enable web filter services. When uploaded to FortiManager, the Web Filter database is displayed.
Enable Email Filter Services	Select to enable email filter services. When uploaded to FortiManager, the Email Filter database is displayed.
Upload Options for FortiGate/FortiMail	
AntiVirus/IPS Packages	Select to upload the FortiGate/FortiMail antivirus and IPS packages. Browse for the file you downloaded from the Customer Service & Support portal on your management computer. Select *OK* to upload the package to FortiManager.
Web Filter Database	Select to upload the web filter database. Browse for the file you downloaded from the Customer Service & Support portal on your management computer. Select *OK* to upload the package to FortiManager.
Email Filter Database	Select to upload the email filter database. Browse for the file you downloaded from the Customer Service & Support portal on your management computer. Select *OK* to upload the package to FortiManager.
Service License	Select to import the FortiGate license. Browse for the file on your management computer. Select *OK* to upload the package to FortiManager.
Upload Options for FortiClient	

AntiVirus/IPS Packages	Select to upload the FortiClient AntiVirus/IPS packages. Browse for the file you downloaded from the Customer Service & Support portal on your management computer. Select *OK* to upload the package to FortiManager.
Service License	Select to import the FortiClient license. Browse for the file on your management computer. Select *OK* to upload the package to FortiManager.

FortiGuard antivirus and IPS settings

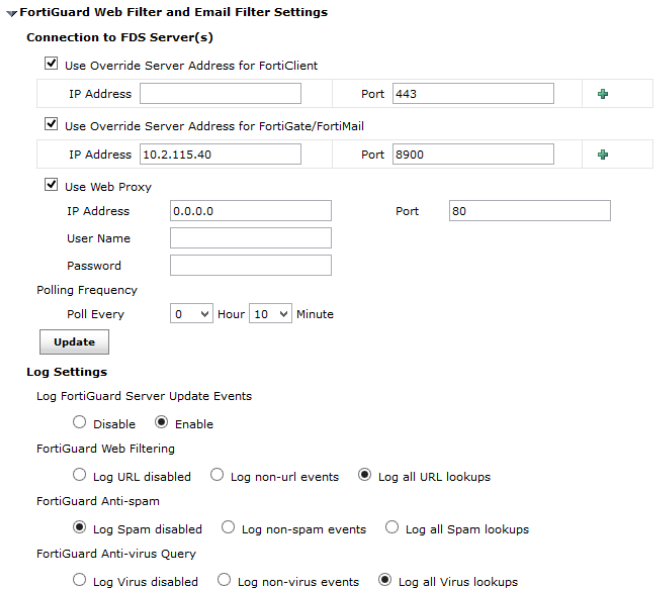
In this section you can enable settings for FortiGuard Antivirus and IPS settings.

Configure the following settings:

Use Override Server Address for FortiGate/FortiMail	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete iconto remove entries. To override the default server for updating FortiGate/FortiMail device's FortiGuard services, see Overriding default IP addresses and ports on page 317.
Allow Push Update	Configure to allow urgent or critical updates to be pushed directly to the FortiManager system when they become available on the FDN. The FortiManager system immediately downloads these updates. To enable push updates, see Enabling push updates on page 316.
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 317.
Scheduled Regular Updates	Configure when packages are updated without manually initiating an update request. To schedule regular service updates, see Scheduling updates on page 318.
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

In this section you can enable settings for FortiGuard Web Filter and Email Filter.



Configure the following settings:

Connection to FDS server(s)	Configure connections for overriding the default built-in FDS or web proxy server for web filter and email filter settings. To override an FDS server for web filter and email filter services, see Overriding default IP addresses and ports on page 317. To enable web filter and email filter service updates using a web proxy server, see Enabling updates through a web proxy on page 317.
Use Override Server Address for FortiClient	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries.
Use Override Server Address for FortiGate/FortiMail	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries. To override the default server for updating FortiGate device's FortiGuard services, see Overriding default IP addresses and ports on page 317.
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 317.

Log Settings	Configure logging of FortiGuard web filtering, email filter, and antivirus query events. • *Log FortiGuard Server Update Events*: enable or disable • *FortiGuard Web Filtering*: Choose from *Log URL disabled*, *Log non-url events*, and *Log all URL lookups*. • *FortiGuard Anti-spam*: Choose from *Log Spam disabled*, *Log non-spam events*, and *Log all Spam lookups*. • *FortiGuard Anti-virus Query*: Choose from *Log Virus disabled*, *Log non-virus events*, and *Log all Virus lookups*. To configure logging of FortiGuard web filtering and email filtering events, see Logging FortiGuard web or email filter events on page 320

Override FortiGuard server (Local FortiManager)

Configure and enable alternate FortiManager FDS devices, rather than using the local FortiManager system. You can set up as many alternate FDS locations, and select what services are used.

Configure the following settings:

Additional number of private FortiGuard servers (excluding this one) (1) +	Select the add icon to add a private FortiGuard server. Select the delete icon to remove entries. When adding a private server, you must type its IP address and time zone.
Enable Antivirus and IPS Update Service for Private Server	When one or more private FortiGuard servers are configured, update anti-virus and IPS through this private server instead of using the default FDN. This option is available only when a private server has been configured.
Enable Web Filter and Email Filter Update Service for Private Server	When one or more private FortiGuard servers are configured, update the web filter and email filter through this private server instead of using the default FDN. This option is available only when a private server has been configured.
Allow FortiGates to access public FortiGuard servers when private servers unavailable	When one or more private FortiGuard servers are configured, managed FortiGate units will go to those private servers for FortiGuard updates. Enable this feature to allow those FortiGate units to then try to access the public FDN servers if the private servers are unreachable. This option is available only when a private server has been configured.

The FortiManager system's network interface settings can restrict which network interfaces provide FDN services. For more information, see Configuring network interfaces on page 69.

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 Management* > *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 316.
3. Select *Apply*.
   The built-in FDS attempts to connect to the FDN. To see the connection status go to *FortiGuard Management* > *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.
Synchronizing	A progress bar appears when the built-in FDS is enabled and is downloading available updates from the FDN.
Synchronized	A green checkmark appears when the built-in FDS is enabled, and FDN package downloads were successfully completed.

If the built-in FDS is unable to connect, you may need to enable the selected services on a network interface. For more information, see Configuring network interfaces on page 69.

If you still cannot connect to the FDN, check routes, DNS, and any intermediary firewalls or NAT devices for policies that block necessary FDN ports and protocols. For additional FDN troubleshooting information, including FDN server selection, see FDN port numbers and protocols on page 318.

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 67.

Matching port settings

When configuring a device to override default FDN ports and IP addresses with that of a FortiManager system, the default port settings for the device's update or query requests may not match the listening port of the FortiManager system's built-in FDS. If this is the case, the device's requests will fail. To successfully connect them, you must match the devices' port settings with the FortiManager system's built-in FDS listening ports.

For example, the default port for FortiGuard antivirus and IPS update requests is TCP 443 on FortiOS v4.0 and higher, but the FortiManager system's built-in FDS listens for those requests on TCP 8890. In this case, the FortiGate unit's update requests would fail until you configure the unit to send requests on TCP 8890.

In some cases, the device may not be configurable; instead, you must configure the FortiManager system to listen on an alternate port.

Handling connection attempts from unregistered devices

The built-in FDS replies to FortiGuard update and query connections from devices registered with the device manager's device list. If the FortiManager is configured to allow connections from unregistered devices, unregistered devices can also connect.

For example, you might choose to manage a FortiGate unit's firmware and configuration locally (from its GUI), but use the FortiManager system when the FortiGate unit requests FortiGuard antivirus and IPS updates. In this case, the FortiManager system considers the FortiGate unit to be an unregistered device, and must decide how to handle the connection attempt. The FortiManager system will handle the connection attempt based on how it is configured. Connection attempt handling is only configurable via the CLI.

To configure connection attempt handling:

1. Go to the CLI console widget in the *System Settings* tab. For information on widget settings, see Customizing the dashboard on page 47.
2. Click inside the console to connect.
3. Type the following CLI command lines 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, type the following CLI command lines:
```
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, type the following CLI command lines:
```
config system admin setting
   set unreg_dev_opt add_no_service
end
```
For more information, see the *FortiManager CLI Reference*.

Configuring FortiGuard services

The FortiGuard Management provides a central location for configuring how the FortiManager system accesses the FDN and FDS, including push updates. The following procedures explain how to configure FortiGuard services and configuring override and web proxy servers, if applicable.

If you need to host a custom URL list that are rated by the FortiGate unit, you can import a list using the CLI.

Enabling push updates

When an urgent or critical FortiGuard antivirus or IPS signature update becomes available, the FDN can push update notifications to the FortiManager system's built-in FDS. The FortiManager system then immediately downloads the update.

To use push update, you must enable both the built-in FDS and push updates. Push update notifications will be ignored if the FortiManager system is not configured to receive them. If TCP port 443 downloads must occur through a web proxy, you must also configure the web proxy connection. See Enabling updates through a web proxy on page 317.

If push updates must occur through a firewall or NAT device, you may also need to override the default push IP address and port.

For example, overriding the push IP address can be useful when the FortiManager system has a private IP address, and push connections to a FortiManager system must traverse NAT. Normally, when push updates are enabled, the FortiManager system sends its IP address to the FDN; this IP address is used by the FDN as the destination for push messages; however, if the FortiManager system is on a private network, this IP address may be a private IP address, which is not routable from the FDN – causing push updates to fail.

To enable push through NAT, type a push IP address override, replacing the default IP address with an IP address of your choice such as the NAT device's external or virtual IP address. This causes the FDN to send push packets to the override IP address, rather than the FortiManager system's private IP address. The NAT device can then forward the connection to the FortiManager system's private IP address.

The built-in FDS may not receive push updates if the external IP address of any intermediary NAT device is dynamic (such as an IP address from PPPoE or DHCP). When the NAT device's external IP address changes, the FortiManager system's push IP address configuration becomes out-of-date.

To enable push updates to the FortiManager system:

1. Go to *FortiGuard Management* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*; see FortiGuard antivirus and IPS settings on page 311.
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, type the IP Address and/or Port number on the NAT device which will forward push packets to the FortiManager system. The FortiManager system will notify the FDN to send push updates to this IP address and port number.
   - *IP Address* is the external or virtual IP address on the NAT device for which you will configure a static NAT or port forwarding.

- *Port* is the external port on the NAT device for which you will configure port forwarding.

5. 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 Management* > *Advanced Settings*.
2. If configuring a web proxy server to enable web and email filtering updates, expand *FortiGuard Web Filter and Email Filter Settings.*
3. If configuring a web proxy to enable antivirus and IPS updates, expand *FortiGuard Antivirus and IPS Settings*.
4. Select the check box beside *Use Web Proxy* and type the IP address and port number of the proxy.
5. If the proxy requires authentication, type the user name and password.
6. 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.
7. 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 Management* > *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 type 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*.

5. Select the appropriate check box beside *Use Override Server Address for FortiGate/FortiMail* and/or *Use Override Server Address for FortiClient* and type the IP address and/or port number.
6. 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.

After connecting to the FDS, you can verify connection status on the FortiGuard Management page. For more information about connection status, see Connecting the built-in FDS to the FDN on page 313.

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 Management* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*; see FortiGuard antivirus and IPS settings on page 311.
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 Management* > *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 321.

Accessing public FortiGuard web and email filter servers

You can configure the FortiManager system to allow the managed FortiGate units to access public FortiGuard web filter or email filter network servers in the event local FortiGuard web filter or email filter server URL lookups fail. You can specify private servers where the FortiGate units can send URL queries.

To access public FortiGuard web and email filter servers:

1. Go to *FortiGuard Management* > *Advanced Settings*.
2. Expand *Override FortiGuard Server (Local FortiManager)*.
3. Select the add icon next to Additional number of private FortiGuard servers (excluding this one) (0). Select the delete icon to remove entries.
4. Type the *IP Address* for the server, and select its *Time Zone*.
5. Repeat step 4 as often as required. You can include up to ten additional servers.
6. Select the additional options to set where the FDS updates come from, and if the managed FortiGate units can access these servers if the local FDS is not available.
   - 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 Management* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*; see FortiGuard antivirus and IPS settings on page 311.
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 Management* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*.
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 Management* > *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).

Licensing status

FortiManager includes a licensing overview page that allows you to view license information for all managed FortiGate devices. To view the licensing status, go to the *FortiGuard* tab and select *Licensing Status* in the tree menu.

This page displays the following information:

Show license expired devices only	Select to display devices with an expired license only.
Refresh	Select the refresh icon to refresh the information displayed on this page.
Search	Use the search field to find a specific device in the table.
Device Name	The device name or host name. You can change the order that devices are listed by clicking the column title.
ADOM	ADOM information. You can change the order that ADOMs are listed by clicking the column title.
Antivirus	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
IPS	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Email Filtering	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Web Filtering	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Support	The license status and expiration date. You can change the order that devices are listed by clicking the column title.

Icon States	• Green: License OK • Orange: License will expire soon • Red: License has expired

Package management

Antivirus and IPS signature packages are managed in *FortiGuard Management* > *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 Management* > *Package Management* > *Receive Status*. This page displays the package received, version, size, to be deployed version, and update history or FortiGate, FortiMail, FortiAnalyzer, and FortiClient.

The following information is displayed:

Refresh	Select to refresh the table.
FortiGuard Connection Status	The FortiGuard connection status.
	The device type: FortiGate, FortiMail, FortiAnalyzer, FortiClient.
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.
Update History	Select the icon to view the package update history.

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.

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 occurred, the statuses of the updates, and the versions downloaded.

Service status

The service status page shows a list of all the managed FortiGate devices, their last update time, and their status. A device's status can be one of the following:

- Up to Date: the latest package has been received by the FortiGate unit.
- Pending: The FortiGate unit has an older version of the package due to an acceptable reason (such as the scheduled update time having not come yet).
- Problem: The FortiGate unit missed the scheduled query, or did not correctly receive the latest package.
- Unknown: The FortiGate unit's status is not currently known.

Pending updates can also be pushed to the devices, either individually or all at the same time. The list can be refreshed by selecting *Refresh* in the toolbar.

This page displays the following:

Push Pending	Select the device in the list and select *Push Pending* in the toolbar to push the update to the device. This option is available in the right-click menu.
Push All Pending	Select *Push All Pending* in the toolbar to push the update to the devices in the list. This option is available in the right-click menu.
Refresh	Select to refresh the list.
Device	The device serial number or host name is displayed.
Status	The service update status. Hover the mouse cursor over a pending icon to view the package to be installed.
Last Update Time	The date and time of the last update.

To push updates to a device or devices:

1. Go to *FortiGuard Management* > *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.
3. 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 Management > Query Server Management > Receive Status*.

The following information is displayed:

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.

Update history

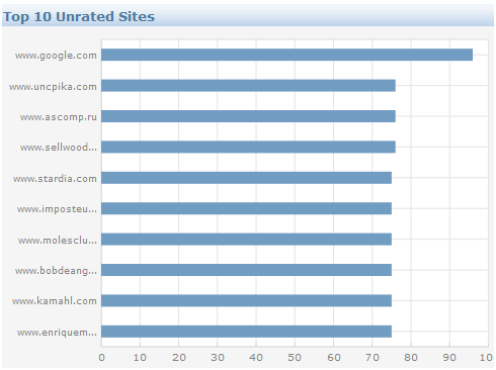
Selecting the update history button for a package opens the update history page for that package.

The following information is displayed:

Date	The date and time of the event.
Event	The event that occurred. One of: Manual Update or Poll Update.
Status	The status of the event.
Download	The version number and size of the download.

Query status

Go to *FortiGuard Management > Query Server Management > Query Status* to view graphs that show: the number of queries made from all managed devices to the FortiManager unit over a user selected time period, the top ten unrated sites, and the top ten devices for a user selected time period.



The following information is displayed:

Top 10 Unrated Sites	Displays the top 10 unrated sites and the number of events. Select the refresh icon to refresh the graph information.
Top 10 Devices	Displays the top 10 devices and number of sessions. Select the edit icon to edit the statistics period. Select a time period from the drop-down list. Select the refresh icon to refresh the graph information.
Number of Queries	Displays the number of queries over a period of time. Select the edit icon to edit the statistics period. Select a time period from the drop-down list. Select the refresh icon to refresh the graph information.

Firmware images

Go to *FortiGuard Management* > *Firmware Images* to manage the firmware images stored on the FortiManager device. You can import firmware images for FortiGate, FortiCarrier, FortiAnalyzer, FortiManager, FortiAP., and FortiExtender.

You can download only those images that are needed from the FDS systems, and customize which firmware images are available for deployment.

The following information and settings are available:

Import Images	Select to open the firmware image import list.
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 firmware image that has been downloaded.

Download/Delete	Download the firmware image from the FDS if it is available. If the firmware images has already been downloaded, then delete the firmware image from the FortiManager device.

For information about upgrading your FortiManager device, see the FortiManager Release Notes or contact Fortinet Customer Service & Support.

To import a firmware image:

1. Go to *FortiGuard Management* > *Firmware Images*. Select *Import Images* in the toolbar.
2. Select a device in the list and select Import in 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 Management* > *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 GUI 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 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.

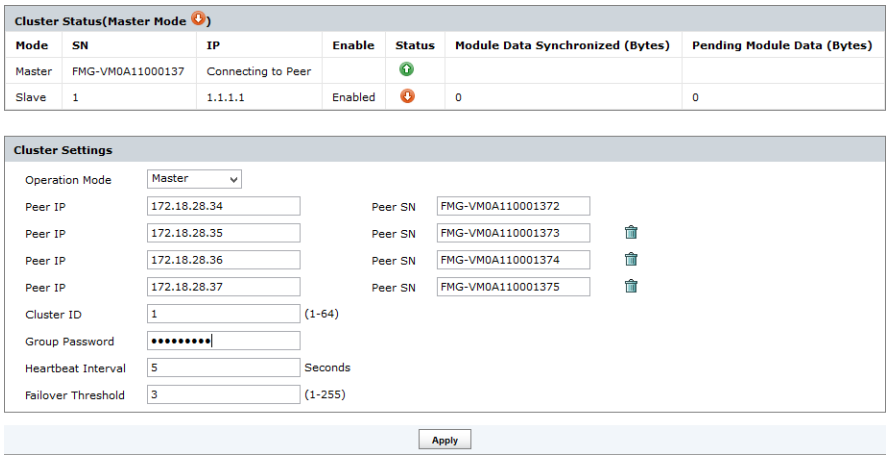
Configuring HA options

To configure HA options go to *System Settings* > *HA*. From here you can configure FortiManager units to start an HA cluster or you can change the HA configuration of the cluster.

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

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

You can connect to the primary unit GUI to work with FortiManager. Because of configuration synchronization you can configure and work with the cluster in the same way as you would work with a standalone FortiManager unit.



Configure the following settings:

Cluster Status	Monitor FortiManager HA status. See Monitoring HA status on page 333.
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	Type 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	Type 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 GUI 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.

GUI configuration steps

Use the following procedures to configure the FortiManager units for HA operation from the FortiManager unit GUI. Sample configuration settings are also shown.

To configure the primary unit for HA operation:

1. Connect to the primary unit GUI.
2. Go to *System Settings* > *HA*.
3. Configure HA settings.

   Example HA master configuration:

Operation Mode	Master
Peer IP	172.20.120.23
Peer SN	<serial_number>
Peer IP	192.268.34.23
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
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 GUI.
2. Go to *System Settings* > *HA*.
3. Configure HA settings.
   Example local backup configuration:

Operation Mode	Slave
Priority	5 (Keep the default setting.)
Peer IP	172.20.120.45
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
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 GUI.
2. Go to *System Settings* > *HA*.
3. Configure HA settings.
   Example remote backup configuration:

Operation Mode	Slave
Priority	5 (Keep the default setting.)
Peer IP	192.168.20.23
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
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* > *HA* to monitor the status of the FortiManager units in an operating HA cluster. The FortiManager HA status dialog box displays information about the role of each cluster unit, the HA status of the cluster, and also displays the HA configuration of the cluster.

The FortiManager GUI browser window title changes to indicate that the FortiManager unit is operating in HA mode. The following text is added to the title *HA (Group ID: <group_id>*). Where <group_id> is the HA Group ID.

From the FortiManager CLI you can use the command `get system ha` to display the same HA status information.

The following information is displayed:

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 GUI or CLI to upgrade the firmware. Then install the firmware on the slave units.

Similar to upgrading the firmware of a standalone FortiManager unit, normal FortiManager operations are temporarily interrupted while the cluster firmware upgrades. As a result of this interruption, you should upgrade the firmware during a maintenance period.

To upgrade FortiManager HA cluster firmware:

1. Log into the primary unit GUI.
2. Upgrade the primary unit firmware.
   The firmware is forwarded to all the slave units, and then all the devices (master and slaves) are rebooted.

   See the *FortiManager Release Notes* and *FortiManager Upgrade Guide* for more information.

Administrators may not be able to connect to the FortiManager GUI until the upgrade synchronization process is complete. During the upgrade, using SSH or telnet to connect to the CLI may also be slow, however use the console to connect to the CLI.

FortiView

The *FortiView* tab allows you to access both FortiView drill down and Log view menus. FortiView in FortiManager collects data from FortiView in FortiGate. In order for information to appear in the FortiView dashboards in FortiGate, disk logging must be selected for the FortiGate unit. Select the FortiView tab and select the ADOM from the drop-down list.

When rebuilding the SQL database, FortiView will not be available until after the rebuild is completed. Select the *Show Progress* link in the message to view the status of the SQL rebuild.

FortiView

Use FortiView o drill down real-time and historical traffic from log devices by sources, applications, destinations, web sites, threats, cloud applications, cloud users, system and admin events, SSL and dialup IPsec, site to site IPsec, rogue APs, and resource usage. Each FortiView summary view can be filtered by a variety of attributes, as well as by device and time period. These attributes can be selected using the right-click context menu. Results can also be filtered using the various columns.

The following summary views are available:

- Top Sources
- Top Applications
- Top Destinations
- Top Web Sites
- Top Threats
- Top Cloud Applications/Users
- System Events
- Admin Logins
- SSL & Dialup IPsec
- Site-to-Site IPsec
- Rogue APs
- Resource usage

Top Sources

The *Top Sources* dashboard displays information about the sources of traffic on your unit. You can drill down the displayed information, select the device and time period, and apply search filters.

The following information is displayed:

Source	Displays the source IP address and/or user name, if applicable. Select the column header to sort entries by source. You can apply a search filter to the source (`srcip`) column.
Device	Displays the device IP address or host name. Select the column header to sort entries by device. You can apply a search filter to the device (`dev_src`) column.
Threat Score (Blocked/Allowed)	Displays the threat score for blocked and allowed traffic. Select the column header to sort entries by threat score.
Sessions (Blocked/Allowed)	Displays the number of sessions blocked and allowed. Select the column header to sort entries by sessions.
Bytes (Sent/Received)	Displays the value for sent and received packets. Select the column header to sort entries by bytes.

The following options are available:

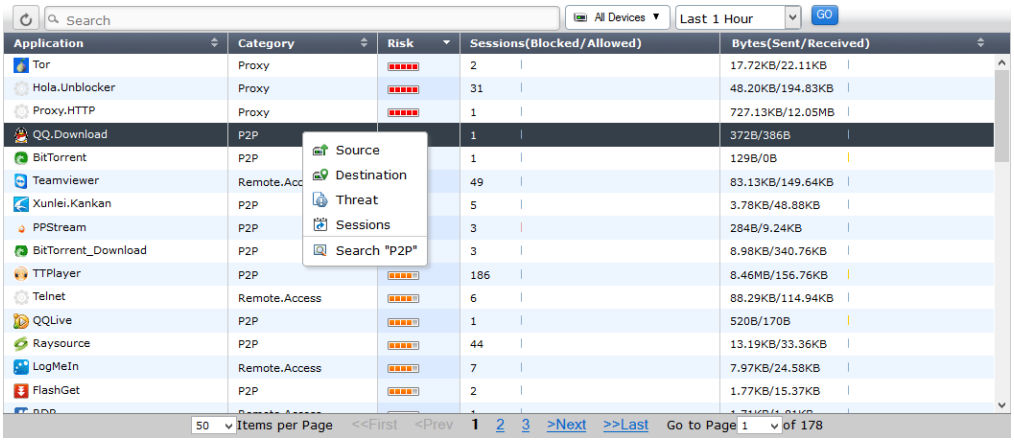
Refresh	Refresh the displayed information.
Search	Click the search field to add a search and select the *GO* button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	

Application	Select to drill down by application to view application related information including the application, number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the application (`app`) column to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Sources* page.
Destination	Select to drill down by destination to view destination related information including the destination IP address and geographic region, the threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`) column to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Sources* page.
Threat	Select to drill down by threat to view threat related information including the threat type, category, threat level, threat score (blocked/allowed), and number of incidents (blocked/allowed). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the threat (`threat`) or category (`threat-type`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Sources* page.
Domain	Select to drill down by domain to view domain related information including domain, category, browsing time, threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. Select the *GO* button to apply the search filter.Select the return icon to return to the *Top Sources* page.
Category	Select to drill down by category to view category related information including category, browsing time, threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Sources* page.
Sessions	Select to drill down by sessions to view session related information including date/time, source/device, destination IP address and geographic region, service, bytes (sent/received), user, application, and security action. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`), service (`service`), user (`user`), or application (`app`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Sources* page.

Search	Add a search filter and select the *GO* button to apply the filter.

Top Applications

The *Top Applications* dashboard shows information about the applications being used on your network, including the application name, category, and risk level. You can drill down the displayed information, select the device and time period, and apply search filters.



The following information is displayed:

Application	Displays the application name and service. Select the column header to sort entries by application. You can apply a search filter to the application (`app`) column.
Category	Displays the application category. Select the column header to sort entries by category. You can apply a search filter to the category (`appcat`) column.
Risk	Displays the application risk level. Hover the mouse cursor over the entry in the column for additional information. Select the column header to sort entries by risk. Risk uses a new 5-point risk rating. The rating system is as follows: • *Critical*: Applications that are used to conceal activity to evade detection. • *High*: Applications that can cause data leakage, are prone to vulnerabilities, or downloading malware. • *Medium*: Applications that can be misused. • *Elevated*: Applications that are used for personal communications or can lower productivity. • *Low*: Business related applications or other harmless applications.
Sessions (Blocked/Allowed)	Displays the number of sessions blocked and allowed. Select the column header to sort entries by sessions.

Bytes (Sent/Received)	Displays the value for sent and received packets. Select the column header to sort entries by bytes.

The following options are available:

Refresh	Refresh the displayed information.
Search	Click the search field to add a search filter and select the *GO* button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Source	Select to drill down by source to view source related information including the source IP address, device MAC address or FQDN, threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the source (`srcip`) and device (`dev_src`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Applications* page.
Destination	Select to drill down by destination to view destination related information including the destination IP address and geographic region, the threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`) column to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Applications* page.

Threat	Select to drill down by threat to view threat related information including the threat type, category, threat level, threat score (blocked/allowed), and number of incidents (blocked/allowed). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the threat (`threat`) or category (`threat-type`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Applications* page.
Sessions	Select to drill down by sessions to view session related information including date/time, source/device, destination IP address and geographic region, service, bytes (sent/received), user, application, and security action. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`), service (`service`), user (`user`), or application (`app`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Applications* page.
Search	Add a search filter and select the *GO* button to apply the filter.

Top Destinations

The *Top Destinations* dashboard shows information about the destination IP addresses of traffic on your FortiGate unit, as well as the application used. You can drill down the displayed information, select the device and time period, and apply search filters.

The following information is displayed:

Destination	Displays the destination IP address and geographic region. A flag icon is displayed to the left of the IP address. Select the column header to sort entries by destination. You can apply a search filter to the destination (`dstip`) column.
Application	Displays the application port and service. When the information displayed exceeds the column width, hover the mouse cursor over the entry in the column for a full list. Select the column header to sort entries by application. You can apply a search filter to the application (`app`) column.
Sessions (Blocked/Allowed)	Displays the number of sessions blocked/allowed. Select the column header to sort entries by sessions.
Bytes (Sent/Received)	Displays the value for sent and received packets. Select the column header to sort entries by bytes.

The following options are available:

Refresh	Refresh the displayed information.

Search	Click the search field to add a search filter and select the *GO* button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Application	Select to drill down by application to view application related information including the service and port, number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the application (`app`) column to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Destinations* page.
Source	Select to drill down by source to view source related information including the source IP address, device MAC address or FQDN, threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the source (`srcip`) and device (`dev_src`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Destinations* page.
Threat	Select to drill down by threat to view threat related information including the threat type, category, threat level, threat score (blocked/allowed), and number of incidents (blocked/allowed). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the threat (`threat`) or category (`threattype`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Destinations* page.

Sessions	Select to drill down by sessions to view session related information including date/time, source/device, destination IP address and geographic region, service, bytes (sent/received), user, application, and security action. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`), service (`service`), user (`user`), or application (`app`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Sources* page.
Search	Add a search filter and select the *GO* button to apply the filter.

Top Web Sites

The *Top Web Sites* dashboard lists the top allowed and top blocked web sites. You can drill down the displayed information, select the device and time period, and apply search filters.

The following information is displayed:

Domain	Displays the domain name. Select the column header to sort entries by domain. You can apply a search filter to the domain (`domain`) column. This column is only shown when *Domain* is selected in the domain/category drop-down list.
Category	Displays the web site category. When the information displayed exceeds the column width, hover the mouse cursor over the entry in the column for a full list. Select the column header to sort entries by category.
Browsing Time	Displays the web site browsing time. Select the column header to sort entries by browsing time.
Threat Score (Blocked/Allowed)	Displays the web site threat score for blocked and allowed traffic. Select the column header to sort entries by threat score.
Sessions (Blocked/Allowed)	Displays the number of sessions blocked and allowed. Select the column header to sort entries by sessions.
Bytes (Sent/Received)	Displays the value for sent and received packets. Select the column header to sort entries by bytes.

The following options are available:

Refresh	Refresh the displayed information.
Search	Click the search field to add a search filter and select the *GO* button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter.

Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Domain/Category	Select to view information based on either the domain or the category.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Source	Select to drill down by source to view source related information including the source IP address, device IP address or FQDN, threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the source (`srcip`) and device (`dev_src`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Web Sites* page.
Destination	Select to drill down by destination to view destination related information including the destination IP address and geographic region, the threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`) column to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Web Sites* page.
Category	Select to drill down by category to view category related information including category, browsing time, threat score (blocked/allowed), number of sessions (blocked/allowed), and bytes (sent/received). You can select to sort entries displayed by selecting the column header. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Web Sites* page.

Threat	Select to drill down by threat to view threat related information including the threat type, category, threat level, threat score (blocked/allowed), and number of incidents (blocked/allowed). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the threat (`threat`) or category (`threattype`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Destinations* page.
Sessions	Select to drill down by sessions to view session related information including date/time, source/device, destination IP address and geographic region, service, bytes (sent/received), user, application, and security action. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`), service (`service`), user (`user`), or application (`app`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Sources* page.
Search	Add a search filter and select the *GO* button to apply the filter.

Top Threats

The *Top Threats* dashboard lists the top users involved in incidents, as well as information on the top threats to your network. You can drill down the displayed information, select the device and time period, and apply search filters.

If you are running FortiOS v5.0.x, you must enable *Client Reputation* in the security profiles on the FortiGate in order to view entries in the *Top Threats* section of FortiView in FortiManager.

The following incidents are considered threats:

- Risk applications detected by application control
- Intrusion incidents detected by IPS
- Malicious web sites detected by web filtering
- Malware/botnets detected by antivirus.

The following information is displayed:

Threat	Displays the threat type. Select the column header to sort entries by threat. You can apply a search filter to the threat (`threat`) column.
Category	Displays the threat category. Select the column header to sort entries by category. You can apply a search filter to the category (`threattype`) column.
Threat Level	Displays the threat level. Select the column header to sort entries by threat level.

Threat Score (Blocked/Allowed)	Displays the threat score for blocked and allowed traffic. Select the column header to sort entries by threat score.
Incidents (Blocked/Allowed)	Displays the number of incidents blocked and allowed. Select the column header to sort entries by incidents.

The following options are available:

Refresh	Refresh the displayed information.
Search	Click the search field to add a search filter and select the *GO* button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Source	Select to drill down by source to view source related information including the source IP address, device MAC address or FQDN, threat score (blocked/allowed), bytes (sent/received), and incidents (blocked/allowed). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the source (`srcip`) and device (`dev_src`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Threats* page.

Destination	Select to drill down by destination to view destination related information including the destination IP address and geographic region, the threat score (blocked/allowed), bytes (sent/received), and incidents (blocked/allowed). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`) column to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Threats* page.
Sessions	Select to drill down by sessions to view session related information including date/time, source/device, destination IP address and geographic region, service, bytes (sent/received), user, application, and security action. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`), service (`service`), user (`user`), or application (`app`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Threats* page.
Search	Add a search filter and select the *GO* button to apply the filter.

Top Cloud Applications/Users

The *Top Cloud Applications/Users* dashboard displays information about the cloud application/user traffic on your FortiGate unit. You can drill down the displayed information, select the device and time period, and apply search filters.

The following information is displayed:

Application	Displays the application name. Select the column header to sort entries by application. You can apply a search filter to the application (`app`) column.
User	Displays the user name. Select the column header to sort entries by user. This column is only shown when *Cloud Users* is selected in the applications/users drop-down list.
Category	Displays the application category. Select the column header to sort entries by category. You can apply a search filter to the category (`appcat`) column. This column is only shown when *Cloud Applications* is selected in the applications/users drop-down list.

Risk	Displays the application risk level. Hover the mouse cursor over the entry in the column for additional information. Select the column header to sort entries by risk. Risk uses a new 5-point risk rating. The rating system is as follows: • *Critical*: Applications that are used to conceal activity to evade detection. • *High*: Applications that can cause data leakage, are prone to vulnerabilities, or downloading malware. • *Medium*: Applications that can be misused. • *Elevated*: Applications that are used for personal communications or can lower productivity. • *Low*: Business related applications or other harmless applications. This column is only shown when *Cloud Applications* is selected in the applications/users drop-down list.
Login IDs	Displays the number of login IDs associated with the application. Select the column header to sort entries by login ID. This column is only shown when *Cloud Applications* is selected in the applications/users drop-down list.
Sessions (Blocked/Allowed)	Displays the number of sessions associated with the application that are blocked or allowed. Select the column header to sort entries by sessions.
File (Up/Down)	Displays the number of files uploaded and downloaded. Hover the mouse cursor over the entry in the column for additional information. Select the column header to sort entries by file.
Videos Played	Displays the number of videos played using the application. Select the column header to sort entries by videos played.
Bytes (Sent/Received)	Displays the value for sent and received packets. Select the column header to sort entries by bytes.

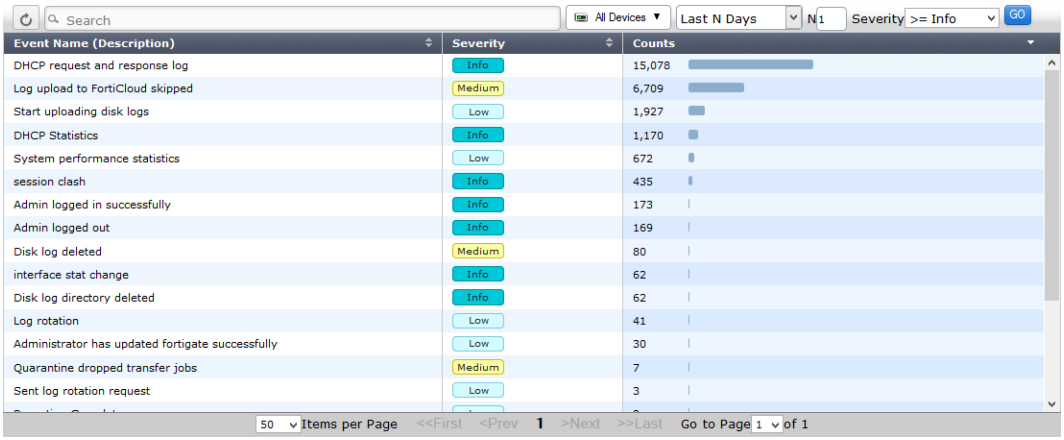
The following options are available:

Search	Click the search field to add a search filter and select the *GO* button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.

Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Cloud Applications / Cloud Users	Select to view information based on either applications or users.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Cloud Users / Cloud Applications	Select to drill down by cloud users to view user related information including IP address, source IP address, number of files uploaded and downloaded, number of videos plays, number of sessions, and bytes (sent/received). You can select to sort entries displayed by selecting the column header. You can apply a search filter in the user (`clouduser`) and source (`source`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Cloud Applications* page.
Files	Select to drill down by files to view file related information including the user email address, source IP address, file name, and file size. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the user (`clouduser`) and source (`srcip`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Cloud Applications* page.
Videos	Select to drill down by videos to view video related information including the user email address, source IP address, file name, and file size. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the user (`clouduser`) and source (`srcip`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Cloud Applications* page.
Sessions	Select to drill down by sessions to view session related information including the date and time, source/device IP address, destination IP address, service, number of packets sent and received, user, application, and security action. You can select to sort entries displayed by selecting the column header. You can apply a search filter in the destination (`dstip`), service (`service`), user (`user`), and application (`app`) columns to further filter the information displayed. Select the *GO* button to apply the search filter. Select the return icon to return to the *Top Cloud Applications* page.
Search	Add a search filter and select the *GO* button to apply the filter.

System Events

The *System Events* dashboard displays an aggregated view of system related events. You can drill down the displayed information, select the device and time period, and apply search filters.



The following information is displayed:

Event Name (Description)	Displays the event log description. Select the column header to sort entries by event name. You can apply a search filter to the Event Name (`event_name`) column.
Severity	Displays the severity level. Select the column header to sort entries by severity.
Counts	Displays the number count. Select the column header to sort entries by count.

The following options are available:

Refresh	Refresh the displayed information.
Search	Click the search field to add a search filter and select the *GO* button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.

Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Severity	Select the severity level from the drop-down list. Select one of the following options: >=Info, >=Low, >=Medium, >=High, or >=Critical.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Log View	Right-click on a column and select *Log View* to view the log entries for the selected entry. Alternatively, double-click the column entry to view the *Log View* page. Select the return icon to return to the *System and Admin* page.
Search	Add a search filter and select the *GO* button to apply the filter.

Admin Logins

The *Admin Login* dashboard displays an aggregated view of admin related events such as admin log in and failed log in attempts. You can drill down the displayed information, select the device and time period, and apply search filters.

The following information is displayed:

User	Displays the administrator user name. Select the column header to sort entries by user. You can apply a search filter to the User (`f_user`) column
Duration	Displays the login duration in seconds. Select the column header to sort entries by duration.
Logins	Displays the number of log ins. Select the column header to sort entries by logins.
Failed Logins	Displays the number of failed log ins. Select the column header to sort entries by failed logins.
Configuration Changes	Displays the number of configuration changes made by the user. Select the column header to sort entries by number of configuration changes.

The following options are available:

Refresh	Refresh the displayed information.

Search	Click the search field to add a search filter and select the *GO* button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Severity	Select the severity level from the drop-down list. Select one of the following options: >=Info, >=Low, >=Medium, >=High, or >=Critical.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Log View	Right-click on a column and select *Log View* to view the log entries for the selected entry. Alternatively, double-click the column entry to view the *Log View* page. Select the return icon to return to the *System and Admin* page.
Search	Add a search filter and select the *GO* button to apply the filter.

SSL & Dialup IPsec

The *SSL and Dialup IPsec* dashboard displays SSL and dialup IPsec VPN events. You can drill down the displayed information, select the device and time period, and apply search filters.

The following information is displayed:

User	Displays the user name connecting to the tunnel. Select the column header to sort entries by user. You can apply a search filter to the user (`f_user`) column.
VPN Type	Displays the VPN type, e.g. ssl-tunnel, ssl-web. You can apply a search filter to the VPN Type (`tunneltype`) column.
Connected From	Displays the connected from IP address.

Number of Connections	Displays the number of connections. Select the column header to sort entries by number of connections.
Duration	Displays the duration the tunnel has been connected. Select the column header to sort entries by duration.
Bytes (Sent/Received)	Displays the value for sent and received packets. Select the column header to sort entries by bytes.

The following options are available:

Refresh	Refresh the displayed information.
Search	Click the search field to add a search filter and select the *GO* button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Dialup Session	Right-click on a column and select *Dialup Session* to view the session related information. Alternatively, double-click the column entry to view the *Dialup Session* page. You can apply a search filter for the Tunnel ID (`tunnelid`) column. Select the return icon to return to the *SSL & Dialup IPsec* page.
Search	Add a search filter and select the *GO* button to apply the filter.

Site-to-Site IPsec

The *Site-to-Site IPsec* dashboard displays site-to-site IPsec VPN events. You can drill down the displayed information, select the device and time period, and apply search filters.

The following information is displayed:

Site-to-Site IPSec Tunnel	Displays the site-to-site VPN tunnel name. You can apply a search filter to the Site-to-Site IPSec Tunnel (`vpntunnel`) column.
Initiating FGT	Displays the initiating IP address.
Connected From	Displays the connected from IP address.
Duration	Displays the duration the tunnel has been connected. Select the column header to sort entries by duration.
Bytes (Sent/Received)	Displays the value for sent and received packets. Select the column header to sort entries by bytes.

The following options are available:

Refresh	Refresh the displayed information.
Search	Click the search field to add a search filter and select the *GO* button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Log View	Right-click on a column and select *Log View* to view the log entries for the selected entry. Alternatively, double-click the column entry to view the *Log View* page. Select the return icon to return to the *Site-to-Site IPsec* page.
Search	Add a search filter and select the *GO* button to apply the filter.

Rogue APs

The Rogue APs dashboard displays rogue AP events. You can drill down the displayed information, select the device and time period, and apply search filters.

The following information is displayed:

SSID	Displays the service set identification (SSID). You can apply a search filter to the SSID (`ssid`) column.
Security Type	Displays the security type, e.g. WPA, WPA2, WPA Auto, Open. You can apply a search filter to the Security Type (`securitymode`) column.
Channel	Displays the channel.
Radio Band	Displays the radio band, e.g. 802.11n, 802.11g.
Vendor Info	Displays the vendor information. You can apply a search filter to the Vendor Info (`manuf`) column.
Total Live Time (HH:MM)	Displays the total live time in the format HH:MM:SS. Select the column header to sort entries by total live time.

The following options are available:

Refresh	Refresh the displayed information.
Search	Click the search field to add a search filter and select the *GO* button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.
N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	

Log View	Right-click on a column and select *Log View* to view the log entries for the selected entry. Alternatively, double-click the column entry to view the *Log View* page. Select the return icon to return to the *Rogue APs* page.
Search	Add a search filter and select the *GO* button to apply the filter.

Resource usage

The Resource Usage dashboard displays device CPU, memory, logging, and other performance information. You can drill down the displayed information, select the device and time period, and apply search filters.

The following information is displayed:

Device Name	Displays the device name. Select the column header to sort entries by device name.
IP Address	Displays the IP address of the device.
CPU Usage	Displays the device CPU usage as a percentage. Select the column header to sort entries by CPU usage.
Memory Usage	Displays the device memory usage as a percentage. Select the column header to sort entries by memory usage.
Logs Per Second	Displays the number of logs per second including the top 3 log types.
Sessions	Displays the number of concurrent sessions for the device. Select the column header to sort entries by sessions.
Bytes	Displays the bytes for the device. Select the column header to sort entries by bytes.

The following options are available:

Refresh	Refresh the displayed information.
Search	Click the search field to add a search filter and select the *GO* button to apply the search filter. Alternatively, you can right-click the column entry to add the search filter.
Devices	Select the device or log array from the drop-down list or select *All Devices*. Select the *GO* button to apply the device filter.
Time Period	Select the time period from the drop-down list. Select *Custom* from the list to specify the start and end date and time. Select the *GO* button to apply the time period filter.

N	When selecting a time period with *last N* in the entry, you can enter the value for N in this text field.
Custom	When *Custom* is selected the custom icon will be displayed. Select the icon to change the custom time period.
Go	Select the *GO* button to apply the filter.
Pagination	Select the number of entries to display per page and browse pages.
Right-click menu	
Resource Usage Drilldown	Right-click on a column and select *Resource Usage Drilldown* to view a graphical representaion of resource usage. Alternatively, double-click the column entry to view the *Resource Usage Drilldown* page. Select the return icon to return to the *Resource Usage* page.
Search	Add a search filter and select the *GO* button to apply the filter.

Log view

Logging and reporting can help you determine what is happening on your network, as well as informing you of certain network activity, such as the detection of a virus, or IPsec VPN tunnel errors. Logging and reporting go hand in hand, and can become a valuable tool for information gathering, as well as displaying the activity that is happening on the network.

Your FortiManager device collects logs from managed FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiSandbox, FortiWeb, FortiClient, and syslog servers.

Device Type	Log Type
FortiGate	Traffic Event: Endpoint, HA, System, Router, VPN, User, WAN Opt. & Cache, and Wireless Security: Vulnerability Scan, AntiVirus, Web Filter, Application Control, Intrusion Prevention, Email Filter, Data Leak Prevention FortiClient VoIP Content logs are also collected for FortiOS 4.3 devices.
FortiCarrier	Traffic, Event
FortiCache	Traffic, Event, Antivirus, Web Filter
FortiClient	Traffic , Event
FortiMail	History, Event, Antivirus, Email Filter

Device Type	Log Type
FortiManager	Event
FortiSandbox	Malware, Network Alerts
FortiWeb	Event, Intrusion Prevention, Traffic
Syslog	Generic

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 Fortinet device system activity, such as when a configuration has changed, or admin login or HA events occur. Event logs are important because they record Fortinet device system activity, which provides valuable information about how your Fortinet unit is performing. The FortiGate event logs includes *System*, *Router*, *VPN*, and *User* menu objects to provide you with more granularity when viewing and searching log data.

Security logs (FortiGate) record all antivirus, web filtering, application control, intrusion prevention, email filtering, data leak prevention, vulnerability scan, and VoIP activity on your managed devices.

The logs displayed on your FortiManager are dependent on the device type logging to it and the features enabled. FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiWeb, FortiSandbox, FortiClient and Syslog logging is supported. ADOMs must be enabled to support non-FortiGate logging.

For more information on logging see the *Logging and Reporting for FortiOS Handbook* in the Fortinet Document Library.

The *Log View* menu displays log messages for connected devices. You can also view, import, and export log files that are stored for a given device, and browse logs for all devices.

When rebuilding the SQL database, Log View will not be available until after the rebuild is completed. Although you can view older logs, new logs will not be inserted into the database until after the rebuild is completed. Select the *Show Progress* link in the message to voew the status of the SQL rebuild.

Viewing log messages

To view log messages, select the *FortiView* tab, select *Log View* in the left tree menu, then browse to the ADOM whose logs you would like to view in the tree menu. You can view the traffic log, event log, or security log information per device or per log array. FortiMail and FortiWeb logs are found in their respective default ADOMs. For more information on FortiGate raw logs, see the *FortiGate Log Message Reference* in the Fortinet Document Library. For more information on other device raw logs, see the *Log Message Reference* for the platform type.

This page displays the following information and options:

Refresh	Select the icon to refresh the log view. This option is only available when viewing historical logs.
Search	Enter a search term to search the log messages. See To perform a text search: on page 363. You can also right-click an entry in one of the columns and select to add a search filter. Select *GO* in the toolbar to apply the filter. Not all columns support the search feature.
Latest Search	Select the icon to repeat previous searches, select favorite searches, or quickly add filters to your search. The filters available will vary based on device and log type.
Clear Search	Select the icon to clear search filters.
Help	Hover your mouse over the help icon, for example search syntax. See Examples on page 363.
Device	Select the device or log array in the drop-down list. Select *Manage Log Arrays* in the *Tools* menu to create, edit, or delete log arrays.
Time Period	Select a time period from the drop-down list. Options include: *Last 30 mins*, *Last 1 hour*, *Last 4 hours*, *Last 12 hours*, *Last 1 day*, *Last 7 days*, *Last N hours*, *Last N days*, or *Custom*. See To customize the time period: on page 363. This option is only available when viewing historical logs.
GO	Select the icon to apply the time period and limit to the displayed log entries. A progress bar is displayed in the lower toolbar.
Custom View	Select to create a new custom view. You can select to create multiple custom views in log view. Each custom view can display a select device or log array with specific filters and time period. See To create a new custom view: on page 362. Custom views are displayed under the *Custom View* menu. This option is only available when viewing historical logs.
Pause | Resume	Pause or resume real-time log display. These two options are only available when viewing real-time logs.
Tools	The tools button provides options for changing the manner in which the logs are displayed, and search and column options. You can manage log arrays and it also provides an option for downloading logs, see Download log messages on page 364.
Real-time Log **Historical Log**	Select to change view from *Real-time Log* to *Historical Log*.
Display Raw	Select to change view from formatted display to raw log display.

	Download	Select to download logs. A download dialog box is displayed. Select the log file format, compress with gzip, the pages to include and select *Apply* to save the log file to the management computer. This option is only available when viewing historical logs in formatted display.
	Manage Log Arrays	Select to create new, edit, and delete log arrays. Once you have created a log array, you can select the log array in the *Device* drop-down menu in the *Log View* toolbar. In FortiManager v5.2.0 and later, when selecting to add a device with VDOMs, all VDOMs are automatically added to the Log Array.
	Case Sensitive Search	Select to enable case sensitive search.
	Enable Column Filter	Select to enable column filters.
Logs		The columns and information shown in the log message list will vary depending on the selected log type, the device type, and the view settings. Right-click on various columns to add search filters to refine the logs displayed. When a search filter is applied, the value is highlighted in the table and log details.
Log Details		Detailed information on the log message selected in the log message list. The item is not available when viewing raw logs. See Log details on page 365 for more information. *Log Details* are only displayed when enabled in the *Tools* menu.
Status Bar		Displays the log view status as a percentage.
Pagination		Adjust the number of logs that are listed per page and browse through the pages.
Limit		Select the maximum number of log entries to be displayed from the drop-down list. Options include: *1000*, *5000*, *10000*, *50000*, or *All*.
Display Log Details		Select the icon to the right of *Limit* to display the log details window.
Archive		Information about archived logs, when they are available. The item is not available when viewing raw logs, or when the selected log message has no archived logs. When an archive is available, the archive icon is displayed. See Archive on page 365 for more information. This option is only available when viewing historical logs in formatted display and when an archive is available.

Customizing the log view

The log message list can show raw or formatted, real time or historical logs. The columns in the log message list can be customized to show only relevant information in your preferred order.

Log display

By default, historical formatted logs are shown in the log message list. You can change the view to show raw logs and both raw and formatted real time logs.

To view real time logs, in the log message list, select *Tools*, then select *Real-time Log* from the drop-down menu. To return to the historical log view, select *Tools*, then select *Historical Log* from the drop-down menu.

To view raw logs, in the log message list, select *View*, then select *Display Raw* from the drop-down menu. To return to the formatted log view, select *Tools*, then select *Display Formatted* from the drop-down menu.

This page displays the following information and options:

Refresh	Select to refresh the log view. This option is only available when viewing historical logs.
Search	Enter a search term to search the log messages. See To perform a text search: on page 363. Select *GO* in the toolbar to apply the filter.
Latest Search	Select the icon to repeat previous searches, select favorite searches, or quickly add filters to your search. The filters available will vary based on device and log type.
Clear Search	Select the icon to clear search filters.
Help	Hover your mouse over the help icon, for example search syntax. See Examples on page 363.
Device	Select the device or log array in the drop-down list. Select *Manage Log Arrays* in the *Tools* menu to create, edit, or delete log arrays.
Time Period	Select a time period from the drop-down list. Options include: *Last 30 mins*, *Last 1 hour*, *Last 4 hours*, *Last 12 hours*, *Last 1 day*, *Last 7 days*, *Last N hours*, *Last N days*, or *Custom*. See To customize the time period: on page 363. This option is only available when viewing historical logs.
GO	Select to apply the time period and limit to the displayed log entries. A progress bar is displayed in the lower toolbar.
Create Custom View	Select to create a new custom view. You can select to create multiple custom views in log view. Each custom view can display a select device or log array with specific filters and time period. See To create a new custom view: on page 362. This option is only available when viewing historical logs.
Pause | Resume	Pause or resume real-time log display. These two options are only available when viewing real-time logs.

Tools		The tools button provides options for changing the manner in which the logs are displayed, and search options. You can manage log arrays and it also provides an option for downloading logs, see Download log messages on page 364.
	Real-time Log Historical Log	Select to change view from *Real-time Log* to *Historical Log*.
	Display Formatted	Select to change view from raw log display to formatted log display.
	Download	Select to download logs. A download dialog box is displayed. Select the log file format, compress with gzip, the pages to include and select *Apply* to save the log file to the management computer. This option is only available when viewing historical logs in formatted display.
	Manage Log Arrays	Select to create new, edit, and delete log arrays. Once you have created a log array, you can select the log array in the *Device* drop-down menu in the *Log View* toolbar.
	Case Sensitive Search	Select to enable case sensitive search.
Detailed Information		Detailed information on the log message selected in the log message list. The item is not available when viewing raw logs.
Status Bar		Displays the log view status as a percentage.
Pagination		Adjust the number of logs that are listed per page and browse through the pages.
Limit		Select the maximum number of log entries to be displayed from the drop-down list. Options include: *1000*, *5000*, *10000*, *50000*, or *All*.

The selected log view will affect the other options that are available in the *View* drop-down menu. Real-time logs cannot be downloaded, and raw logs to not have the option to customize the columns.

Columns

The columns displayed in the log message list can be customized and reordered as needed. Filters can also be applied to the data in a column.

To customize the displayed columns:

1. In the log message list, right-click on a column heading. The *Column Settings* pop-up menu opens.
2. Select a column to hide or display, select *Reset to Default* to reset to the default columns, or select *More Columns* to open the *Column Settings* window.

The available column settings will vary based on the device and log type selected.

a. In the Column Settings window, multiple columns can be added or removed as required, and the order of the displayed columns can be adjusted by dragging and dropping the column names.
b. To reset to the default columns, select *Reset to Default*.

3. Select *OK* to apply your changes.

To filter column data:

1. In the log message list, select *Tools*, then select *Enable Column Filter* from the drop-down menu to enable column filters.
2. In the heading of the column you need to filter, select the filter icon. The filter icon will only be shown on columns that can filtered.

   The *Filter Settings* dialog box opens.
3. Enable the filter, then enter the required information to filter the selected column. The filter settings will vary based on the selected column.
4. Select *Apply* to apply the filter to the data.

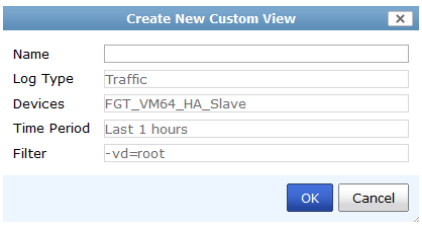
   The column's filter icon will turn green when the filter is enabled, Downloading the current view will only download the log messages that meet the current filter criteria.

Custom views

Select *Create Custom View* in the toolbar to create a new custom log view. Use *Custom View* to save a custom search, device selection, and time period so that you can select this view at any time to view results without having to re-select these criteria. Custom views are listed under the *Custom View* menu and allow you to quickly view log data based on specific time and content filters without having to re-configure filters.

To create a new custom view:

1. In the *Log View* pane, select a log type.
2. Enter a search term, select a device or devices, select a time period, limit the number of logs to display as needed, then select *Custom View*. The *Create New Custom View* dialog box is displayed.



3. Enter a name for the new custom view. All other fields are read-only. The new custom view is saved to the Custom View folder in the ADOM.

To edit a custom view:

1. In the *Log View* pane, select the *Custom View* folder in the tree menu.
2. Select the custom view you would like to edit.
3. Edit the custom search, devices, time period, limit the number of logs to display, and select *GO*.
4. Right-click the name of the custom view and select *Save* to save your changes.

To rename a custom view:

1. In the *Log View* pane, select an ADOM, and select the Custom View folder.
2. Right-click the name of the custom view and select *Rename* in the menu. The *Rename Custom View* dialog box opens.
3. Edit the name and select *OK* to save your changes.

To delete a custom view:

1. In the *Log View* pane, select an ADOM, and select the Custom View folder.
2. Right-click the name of the custom view and select *Delete* in the menu.
3. Select *OK* in the confirmation dialog box to delete the view.

Searching log messages

Log messages can be searched based on a text string and/or time period. Recent searches can be quickly repeated, a time period can be specified or customized, and the number of displayed logs can be limited. A text string search can be case sensitive or not as required.

To perform a text search:

1. In the log message list, select *Tools*, then either select or deselect *Case Sensitive Search* from the drop-down menu to enable or disable case sensitivity in the search string.
2. In the log message list, enter a text string in the search field in the following ways:
   - Manually type in the text that you are searching for. Wildcard characters are accepted.
   - Right-click on the element in the list that you would like to add to the search and select to search for strings that either match or don't match that value.
   - Select a previous search or default filter, using the history icon. The available filters will vary depending on the selected log type and displayed columns.
   - Paste a saved search into the search field.
3. Select *GO* to search the log message list.

To customize the time period:

1. In the log message list, open the time period drop-down menu, and select *Custom...*. The *Custom Timeframe* dialog box opens.
2. Specify the desired time period using the *From* and *To* fields, or select *Any Time* to remove any time period from the displayed data.
3. Select *Apply* to create the custom time period. A calendar icon will be shown next to the time period drop-down list. Select it to adjust the custom time period settings.
4. Select *GO* to apply your settings to the log message list.

Examples

To view example text search strings, hover your cursor over the help icon.

The first example will search for log messages with a source IP address of 172.16.86.11 and a service of HTTP. Because it is not specified, the and operator is assumed, meaning that both conditions must be met for the log message to be included in the search results.

The second example will search for any log messages with source IP addresses that start with either 172.16 or 172.18. Notice the use of the * wildcard. The use of the *or* operator means that either condition can be met for the log message to be included in the search results.

The third example will search for any log message that do not have a source IP address of 172.16.86.11 and a service of HTTP. The use of the *and* operator means that both conditions must be met for the log message to be excluded from the search results.

Download log messages

Log messages can be downloaded to the management computer as a text or CSV file. Real time logs cannot be downloaded.

To download log messages:

1. In the log message list, select *Tools*, then select *Download*. The *Download* dialog box opens.
2. Select a log format from the drop down list, either *Text* or *CSV*.
3. Select *Compress with gzip* to compress the downloaded file.
4. Select *Current Page* to download only the current log message page, or *All Pages* to download all of the pages in the log message list.
5. Select *Apply* to download the log messages to the management computer.

Log arrays

Log Array has been relocated to *Log View* in the *FortiView* tab from the *Device Manager* tab. Upon upgrading to FortiManager v5.2.0 and later, all previously configured log arrays will be imported. In FortiManager v5.0.6 and earlier, when creating a Log Array with both devices and VDOMs, you need to select each device and VDOM to add it to the Log Array. In FortiManager v5.2.0 and later, when selecting to add a device with VDOMs, all VDOMs are automatically added to the Log Array.

To create a new log array:

1. In the *Log View* pane, select the *Tools* button, and select *Manage Log Arrays*. The *Manage Log Arrays* dialog box opens.
2. Select *Create New* in the dialog box toolbar. The *Create New Log Array* dialog box opens.
3. Enter the following:

Name	Enter a unique name for the log array.
Comments	Enter optional comments for the log array.
Devices	Select the add icon and select devices and VDOMs to add to the log array. Select *OK* in the device selection window.

4. Select *OK* to create the new log array.
5. Select the close icon to close the *Manage Log Arrays* dialog box.

To edit a log array:

1. In the *Log View* pane, select *Tools*, and select *Manage Log Arrays*. The *Manage Log Arrays* dialog box is displayed.
2. Select a log array entry and select *Edit* in the toolbar. The *Edit Log Array* dialog box is displayed.
3. Edit the log array name, comments, and devices as needed.
4. Select *OK* to save the log array.
5. Select the close icon to close the *Manage Log Arrays* dialog box.

To delete a log array:

1. In the *Log View* pane, select *Tools*, and select *Manage Log Arrays*. The *Manage Log Arrays* dialog box is displayed.
2. Select the log array entry and select *Delete* in the toolbar.
3. Select *OK* in he confirmation dialog box to delete the log array.
4. Select the close icon to close the *Manage Log Arrays* dialog box.

Log details

Log details can be viewed for any of the collected logs. The details provided in vary depending on the device and type of log selected. The fields available in the this pane cannot be edited or re-organized.

To view log details, select the log in the log message list. Click the log details icon to the left of the limit field, the log details frame will be displayed in the lower frame of the content pane. Log details are not available when viewing raw logs.

In the *Log View* pane, select the *Tools* button, and select *Display Log Details* to enable log details display.

Archive

The *Archive* tab is displayed next to the *Log Details* tab in the lower content pane when archived logs are available. The archive icon is displayed in the log entry line to identify that an archive file is available.

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.

Browsing log files

Go to *FortiView* > *Log View* > *Log Browse* to view log files stored for devices. In this page you can display, download, delete, and import log files.

When a log file reaches its maximum size or a 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 logs on page 371.

If you display the log messages in formatted view, you can perform all the same actions as with the log message list. See Viewing log messages on page 357.

This page displays the following:

Delete	Select the file of files whose log messages you want to delete, then select *Delete*, and then select *OK* in the confirmation dialog box.
Display	Select the file whose log messages you want to view, then select *Display* to open the log message list. For more information, see Viewing log messages on page 357
Download	Download a log file. See Downloading a log file on page 367.
Import	Import log files. See Importing a log file on page 367.
Search	Search the log files by entering a text value in the search window, such as a device serial number.
Log file list	A list of the log files.
Device	The device host name.
Serial Number	The device serial number.
Type	The log type. For example: *Email Filter*, *Event*, *Traffic*, *Web Filter*, *Virus*, *Application Control*, *Data Leak Prevention*, etc.
Log Files	A list of available log files for each device. 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 time when the log file began to be generated.
To	The time when the log file generation ended.

Size (bytes)	The size of the log file, in bytes.
Pagination	Adjust the number of logs that are listed per page and browse through the pages.

Importing a log file

Imported 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 the log files. If you back up the log files, after changing the RAID configuration, you can import the logs to restore them to the FortiManager unit.

To import a log file:

1. Go to *FortiView > Log View > Log Browse*.
2. Select *Import* in the toolbar. The *Import Log File* dialog box opens.
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, select *Browse*. and find to the log file on the management computer.
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 has been successfully uploaded, the FortiManager unit will inspect the 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.

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 log file:

1. Go to *FortiView > Log View > Log Browse*.
2. Select the specific log file that you need to download, then select *Download* from the toolbar. The *Download Log File* dialog box opens.
3. Select the log file format, either text, Native, or CSV.
4. Select *Compress with gzip* to compress the log file.
5. Select *Apply* to download the log file.

   If prompted by your web browser, select a location to where save the file, or open the file without saving.

FortiClient logs

The FortiManager unit can receive FortiClient logs uploaded through TCP port 514. FortiClient logs can be viewed in *FortiView* > *Log View* under the FortiGate device that FortiClient is registered to. Both traffic and event logs are available. Logs can be viewed in both historical and real-time views and in both formatted and raw log views.

In FortiManager v5.2.1 and later, log injection into the SQL database is supported for v5.2 or later licensed endpoints. Clients with the v5.0 license are able to send logs to FortiManager, but these logs will not be inserted into the SQL database.

The following information is displayed:

Traffic logs	The following columns are supported by default for event logs: Date/Time, Device ID, FGT Serial, Source, Source IP, Remote IP, Remote Name, URL, User, and Security Action. Click the log details icon to the left of the limit field to view additional log information. Click the column header to set column settings. Select *More Columns* for additional columns. Right-click the column field to apply a search filter. Not all columns support this feature.
Event logs	The following columns are supported by default for event logs: Date/Time, Device ID, FGT Serial, User, Client Feature, Action, and Message. Click the log details icon to the left of the limit field to view additional log information. Click the column header to set column settings. Select *More Columns* for additional columns. Right-click the column field to apply a search filter. Not all columns support this feature.
Vulnerability Scan logs	The following columns are supported by default for event logs: Date/Time, UID, Device ID, User, vulnname, vulnseverity, and Vulnerability Category. Click the log details icon to the left of the limit field to view additional log information. Click the column header to set column settings. Select *More Columns* for additional columns. Right-click the column field to apply a search filter. Not all columns support this feature.

To download a FortiClient log file, select the desired log from the list, then select *Download* from the Tools menu. In the confirmation dialog box, select if you want to compress the log file with gzip, then select *Apply* to download the log file.

For more information, see the *FortiClient Administration Guide*.

FortiMail logs

The FortiManager unit can receive logs from a FortiMail. FortiMail logs can be viewed in *FortiView* > *Log View*. Logs can be viewed in both historical view and in both formatted and raw log views.

The following information is displayed:

History logs	The following columns are supported by default for event logs: Date/Time, Device ID, Direction, Mailer, From To, Virus, Client Name, Destination IP, Disposition, Classifier, Session ID, Subject, Message Length, Resolved, Policy ID, and Domain. Click the log details icon to the left of the limit field to view additional log information. Click the column header to set column settings. Select *More Columns* for additional columns. Right-click the column field to apply a search filter. Not all columns support this feature.
Event logs	The following columns are supported by default for event logs: Date/Time, Device ID, Sub Type, Session ID, and Message. Click the log details icon to the left of the limit field to view additional log information. Click the column header to set column settings. Select *More Columns* for additional columns. Right-click the column field to apply a search filter. Not all columns support this feature.
AntiVirus logs	The following columns are supported by default for event logs: Date/Time, Device ID, From, To, Source, Message, and Session ID. Click the log details icon to the left of the limit field to view additional log information. Click the column header to set column settings. Select *More Columns* for additional columns. Right-click the column field to apply a search filter. Not all columns support this feature.
Email Filterlogs	The following columns are supported by default for event logs: Date/Time, Device ID, From, To, Message, Client Name, Subject, Destination IP, and Session ID. Click the log details icon to the left of the limit field to view additional log information. Click the column header to set column settings. Select *More Columns* for additional columns. Right-click the column field to apply a search filter. Not all columns support this feature.

FortiManager logs

The FortiManager unit can receive logs from a FortiManager. FortiManager logs can be viewed in *FortiView* > *Log View*. Logs can be viewed in both historical view and in both formatted and raw log views.

The following information is displayed:

Event logs	The following columns are supported by default for event logs: Date/Time, Device ID, Sub Type, Level, User, and Message. Click the log details icon to the left of the limit field to view additional log information. Click the column header to set column settings. Select *More Columns* for additional columns. Right-click the column field to apply a search filter. Not all columns support this feature.

FortiSandbox logs

The FortiManager unit can receive logs from a FortiSandbox. FortiSandbox logs can be viewed in *FortiView* > *Log View*. Logs can be viewed in both historical view and in both formatted and raw log views.

The following information is displayed:

Malware logs	The following columns are supported by default for event logs: Date/Time, Level, Risk, Malware Name, Source IP, and Destination IP. Click the log details icon to the left of the limit field to view additional log information. Click the column header to set column settings. Select *More Columns* for additional columns. Right-click the column field to apply a search filter. Not all columns support this feature.
Network Alerts logs	The following columns are supported by default for event logs: Date/Time, Level, Destination IP:Port, Attack Name, and Host. Click the log details icon to the left of the limit field to view additional log information. Click the column header to set column settings. Select *More Columns* for additional columns. Right-click the column field to apply a search filter. Not all columns support this feature.

FortiWeb logs

The FortiManager unit can receive logs from a FortiWeb. FortiWeb logs can be viewed in *FortiView* > *Log View*. Logs can be viewed in both historical view and in both formatted and raw log views.

The following information is displayed:

Event logs	The following columns are supported by default for event logs: Date/Time, Device ID, Level, User Interface, Action, and Message. Click the log details icon to the left of the limit field to view additional log information. Click the column header to set column settings. Select *More Columns* for additional columns. Right-click the column field to apply a search filter. Not all columns support this feature.
Intrusion Prevention logs	The following columns are supported by default for event logs: Date/Time, Device ID, Source, Destination, Policy, Action, HTTP URL, HTTP Host, and Message. Click the log details icon to the left of the limit field to view additional log information. Click the column header to set column settings. Select *More Columns* for additional columns. Right-click the column field to apply a search filter. Not all columns support this feature.

Traffic logs	The following columns are supported by default for event logs: Date/Time, Device ID, Service, Source, Destination, Policy, HTTP Method, HTTP RETCODE, and Message. Click the log details icon to the left of the limit field to view additional log information. Click the column header to set column settings. Select *More Columns* for additional columns. Right-click the column field to apply a search filter. Not all columns support this feature.

Syslog server logs

The FortiManager unit can receive logs from a syslog server. Syslog logs can be viewed in *FortiView* > *Log View* > *Syslog*. Event logs are available. Logs can be viewed in both historical and real-time views and in both formatted and raw log views.

The following information is displayed:

Syslog logs	The following columns are supported by default for event logs: Date/Time, Device ID, Level, and Message. Click the log details icon to the left of the limit field to view additional log information. Click the column header to set column settings. Select *More Columns* for additional columns. Right-click the column field to apply a search filter. Not all columns support this feature.

Configuring rolling and uploading of logs

You can control device log file size and use of the FortiManager unit's disk space by configuring log rolling and scheduled uploads to a server.

As the FortiManager unit receives new log items, it performs the following tasks:

- verifies whether the log file has exceeded its file size limit
- checks to see if it is time to roll the log file if the file size is not exceeded.

Configure the time to be either a daily or weekly occurrence, and when the roll occurs. When a current log file (`tlog.log`) reaches its maximum size, or reaches the scheduled time, the FortiManager unit rolls the active log file by renaming the file. The file name will be in the form of `xlog.N.log` (for example, `tlog.1252929496.log`), where `x` is a letter indicating the log type and `N` is a unique number corresponding to the time the first log entry was received. The file modification time will match the time when the last log was received in the log file.

Once the current log file is rolled into a numbered log file, it will not be changed. New logs will be stored in the new current log called `tlog.log`. If log uploading is enabled, once logs are uploaded to the remote server or downloaded via the GUI, they are in the following format:

```
FG3K6A3406600001-tlog.1252929496.log-2012-09-29-08-03-54.gz
```

If you have enabled log uploading, you can choose to automatically delete the rolled log file after uploading, thereby freeing the amount of disk space used by rolled log files. If the log upload fails, such as when the FTP server is unavailable, the logs are uploaded during the next scheduled upload.

Log rolling and uploading can be enabled and configured in the GUI in S*ystem Settings* > *Advanced* > *Device Log Settings*. For more information, see Device log settings on page 119. Log rolling and uploading can also be enabled and configured using the CLI. For more information, see the *FortiManager CLI Reference*.

To enable or disable log file uploads:

To enable log uploads, enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set upload enable
      end
   end
```

To disable log uploads, enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set upload disable
      end
   end
```

To roll logs when they reach a specific size:

Enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set file-size <integer>
      end
   end
```

where `<integer>` is the size at which the logs will roll, in MB.

To roll logs on a schedule:

To disable log rolling, enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set when none
      end
   end
```

To enable daily log rolling, enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set upload enble
      set when daily
      set hour <integer>
      set min <integer>
      set file-size <integer>
      end
   end
```

where:

`hour` is the hour of the day when the when the FortiManager rolls the traffic analyzer logs,

`min` is the minute when the FortiManager rolls the traffic analyzer logs, and

`file-size` is the size of the log files at which the logs will roll.

To enable weekly log rolling, enter the following CLI commands:

```
config system log settings
   config rolling-regular
      set when weekly
      set days {mon | tue | wed | thu | fri | sat | sun}
      set hour <integer>
      set min <integer>
      end
   end
```

where:

`days` is the days week when the FortiManager rolls the traffic analyzer logs,

`hour` is the hour of the day when the when the FortiManager rolls the traffic analyzer logs, and

`min` is the minute when the FortiManager rolls the traffic analyzer logs.

Event Management

In the Event Management tab you can configure events handlers based on log type and logging filters. You can select to send the event to an email address, SNMP community, or syslog server. Events can be configured per device, for all devices, or for the local FortiManager. You can create event handlers for FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiWeb, FortiSandbox devices, and syslog servers. In v5.2.0 or later, Event Management supports local FortiManager event logs.

Events can also be monitored, and the logs associated with a given event can be viewed.

When rebuilding the SQL database, Event Management will not be available until after the rebuild is completed. Select the *Show Progress* link in the message to view the status of the SQL rebuild.

Events

The events page provides a list of the generated events. Right-clicking on an event in the table gives you the option of viewing event details including the raw log entries associated with that event, adding review notes, and acknowledging the event.

To view events, go to the *Event Management* tab and select *Event Management* > *All Events*. You can also view events by severity and by handler. When ADOMs are enabled, select the ADOM, and then select *All Events*.

The following information is displayed:

Count	The number of log entries associated with the event. Click the heading to sort events by count.
Event Name	The name of the event. Click the heading to sort events by event name.
Severity	The severity level of the event. Event severity level is a user configured variable. The severity can be *Critical*, *High*, *Medium*, or *Low*. Click the heading to sort events by severity.
Event Type	The event type. For example, *Traffic* or *Event*. Click the heading to sort events by event type. IPS and Application Control event names are links. Select the link to view additional information.
Additional Info	Additional information about the event. Click the heading to sort events by additional information.
Last Occurrence	The date and time that the event was created and added to the events page. Click the heading to sort events by last occurrence.
Pagination	Adjust the number of logs that are listed per page and browse through the pages.

The following options are available:

Refresh	Select to refresh the entries displayed.
Time Period	Select a time period from the drop-down list. Select one of: *Last 30 mins*, *Last 1 hour*, *Last 4 hours*, *Last 12 hours*, *Last 1 day*, *Last 7 days*, *Last N hours*, *Last N days*, *All*. If applicable, enter the number of days or hours for N in the *N* text box.
Show Acknowledged	Select to show or hide acknowledged events. Acknowledged events are greyed out in the list.
Search	Search for a specific event.
View Details	The *Event Details* page is displayed. This option is available in the right-click menu.
Acknowledge	Acknowledge an event. If *Show Acknowledge* is not selected, the event will be hidden. This option is available in the right-click menu.

Event details

Event details provides a summary of the event including the event name, severity, type, count, additional information, last occurrence, device, event handler, raw log entries, and review notes. You can also acknowledge and print events in this page.

To view log messages associated with an event:

1. In the events list, either double-click on an event or right-click on an event then select *View Details* in the right-click menu. The *Event Details* page opens.
2. The following information and options are available:

Print	Select the print icon to print the event details page. The log details pane is not printed.
Return	Select the return icon to return to the *All Events* page.
Event Name	The name of the event, also displayed in the title bar.
Severity	The severity level configured for the event handler.
Type	The event category of the event handler.
Count	The number of logged events associated with the event.
Additional Info	This field either displays additional information for the event or a link to the FortiGuard Encyclopedia. A link will be displayed for AntiVirus, Application Control, and IPS event types.
Last Occurrence	The date and time of the last occurrence.

Device	The device hostname associated with the event.
Event Handler	The name of the event handler associated with the event. Select the link to edit the event handler.
Text box	Optionally, you can enter a 1023 character comment in the text field. Select the save icon to save the comment, or cancel to cancel your changes.
Logs	The logs associated with the log event are displayed. The columns and log fields are dependent on the event type.
Pagination	Adjust the number of logs that are listed per page and browse through the pages.
Log details	Log details are shown in the lower content pane for the selected log. The details will vary based on the log type.

3. Select the return icon to return to the *All Events* page.

Acknowledge events

You can select to acknowledge events to remove them from the event list. An option has been added to this page to allow you to show or hide these acknowledged events.

To acknowledge events:

1. From the event list, select the event or events that you would like to acknowledge.
2. Right-click and select *Acknowledge* in the right-click menu.
3. Select the *Show Acknowledge* checkbox in the toolbar to view acknowledged events.

Event handler

The event handler allows you to view, create new, edit, delete, clone, and search event handlers. You can select these options in the toolbar. The right-click menu includes these options and also includes the ability to enable or disable configured event handlers. You can create event handlers for a specific device, multiple devices, or the local FortiManager. You can select to create event handlers for traffic logs or event logs.

FortiManager v5.2.0 or later includes default event handlers for FortiGate and FortiCarrier devices. Click on the event handler name to enable or disable the event handler and to assign devices to the event handler.

Event Handler	Description
Antivirus Event	• Severity: High • Log Type: Traffic Log • Event Category: AntiVirus • Group by: Virus Name • Log messages that match all conditions: • *Level Greater Than or Equal To Information*

App Ctrl Event	• Severity: Medium
	• Log Type: Traffic Log
	• Event Category: Application Control
	• Group by: Application Name
	• Log messages that match any of the following conditions:
	  • *Application Category Equal To Botnet*
	  • *Application Category Equal To Proxy*

Conserve Mode	• Severity: Critical • Log Type: Event Log • Event Category: System • Group by: Message • Log messages that match all conditions: • *Log Description Equal To System services entered conserve mode*
DLP Event	• Severity: Medium • Log Type: Traffic Log • Event Category: DLP • Group by: DLP Rule Name • Log messages that match all conditions: • *Security Action Equal To Blocked*
HA Failover	• Severity: Medium • Log Type: Event Log • Event Category: HA • Group by: Log Description • Log messages that match all conditions: • *Log Description Equal To Virtual cluster move member*

Event Handler	Description

Interface Down	• Severity: High
	• Log Type: Event Log
	• Event Category: System
	• Group by: Message
	• Log messages that match all conditions:
	  • *Action Equal To interface-stat-change*
	  • *Status Equal To DOWN*

Interface Up	• Severity: Medium
	• Log Type: Event Log
	• Event Category: System
	• Group by: Message
	• Log messages that match all conditions:
	  • *Action Equal To interface-stat-change*
	  • *Status Equal To UP*

IPS - Critical Severity	• Severity: Critical • Log Type: IPS • Group by: Attack Name • Log messages that match all conditions: • *Severity Equal To Critical*
IPS - High Severity	• Severity: High • Log Type: IPS • Group by: Attack Name • Log messages that match all conditions: • *Severity Equal To High*
IPS - Medium Severity	• Severity: Medium • Log Type: IPS • Group by: Attack Name • Log messages that match all conditions: • *Severity Equal To Medium*
IPS - Low Severity	• Severity: Low • Log Type: IPS • Group by: Attack Name • Log messages that match all conditions: • *Severity Equal To Low*

Event Handler	Description
IPsec Phase2 Down	• Severity: Medium • Log Type: Event Log • Event Category: VPN • Group By: VPN Tunnel • Log messages that match all conditions: • *Action Equal To phase2-down*
IPsec Phase2 Up	• Severity: Medium • Log Type: Event Log • Event Category: VPN • Group By: VPN Tunnel • Log messages that match all conditions: • *Action Equal To phase2-up*
Local Device Event	• Devices: Local FortiManager • Severity: Medium • Log Type: Event Log • Event Category: Endpoint • Log messages that match all conditions: • *Level Greater Than or Equal To Warning*

Power Supply Failure	• Severity: Critical
	• Log Type: Event Log
	• Event Category: System
	• Group by: Message
	• Log messages that match any of the following conditions:
	  • *Action Equal To power-supply-monitor*
	  • *Status Equal To failure*

UTM Antivirus Event	• Severity: High • Log Type: Virus • Group by: Virus Name • Log messages that match all conditions: • *Level Greater Than or Equal To Information*

UTM App Ctrl Event	• Severity: Medium
	• Log Type: Application Control
	• Group by: Application Name
	• Log messages that match any of the following conditions:
	  • *Application Category Equal To Botnet*
	  • *Application Category Equal To Proxy*

Event Handler	Description
UTM DLP Event	• Severity: Medium • Log Type: DLP • Group by: DLP Rule Name • Log messages that match all conditions: • *Action Equal To Block*
UTM Web Filter Event	• Severity: Medium • Log Type: Web Filter • Group by: Category • Log messages that match any of the following conditions: • *Web Category Equal To Child Abuse*, *Discrimination*, *Drug Abuse*, *Explicit Violence*, *Extremist Groups*, *Hacking*, *Illegal or Unethical*, *Plagiarism*, *Proxy Avoidance*, *Malicious Websites*, *Phishing*, *Spam URLs*
Web Filter Event	• Severity: Medium • Log Type: Traffic Log • Event Category: WebFilter • Group by: Category • Log messages that match any of the following conditions: • *Web Category Equal To Child Abuse*, *Discrimination*, *Drug Abuse*, *Explicit Violence*, *Extremist Groups*, *Hacking*, *Illegal or Unethical*, *Plagiarism*, *Proxy Avoidance*, *Malicious Websites*, *Phishing*, *Spam URLs*

The Antivirus Event, App Ctrl Event, and DLP Event handlers are not supported by FortiOS 5.2.

Go to the *Event Management* tab and select *Event Handler* in the tree menu.

The following information is displayed:

Status	The status of the event handler (enabled or disabled).
Name	The name of the event handler.
Filters	The filters that are configured for the event handler.
Event Type	The event category of the event handler. The information displayed is dependent on the platform type.

Devices	The devices that you have configured for the event handler. This field will either display *All Devices* or list each device. When you have configured an event handler for local logs, *Local FortiManager* will be displayed. *Local FortiManager* is available in the root ADOM only and is used to query FortiManager event logs.
Severity	The severity that you configured for the event handler. This field will display *Critical, High, Medium*, or *Low*.
Send Alert to	The email address, SNMP server, or syslog server that has been configured for the event handler.

Right-click on an event handler in the list to open the right-click menu. The following options are available:

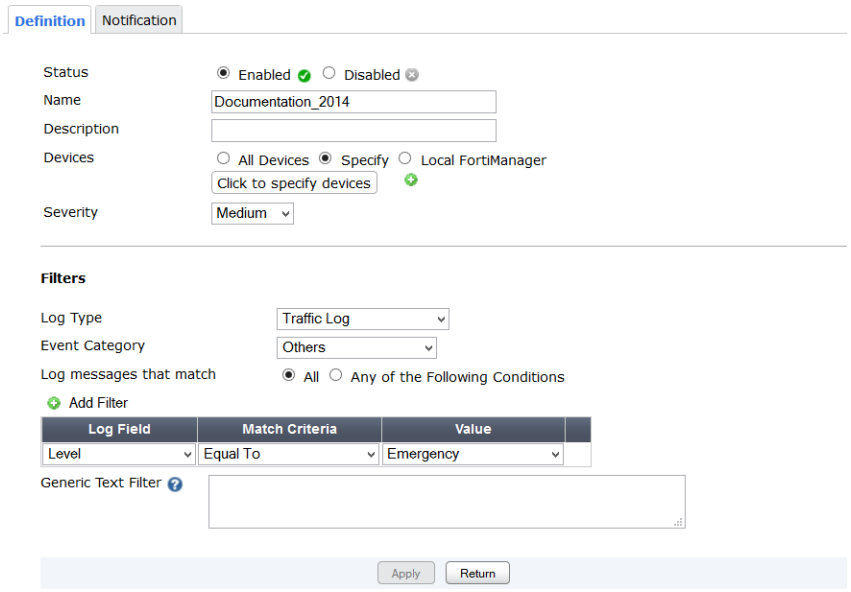
Create New	Select to create a new event handler. This option is available in the toolbar and right-click menu.
Edit	Select an event handler and select edit to make changes to the entry. This option is available in the toolbar and right-click menu.
Delete	Select one or all event handlers and select delete to remove the entry or entries. This option is available in the toolbar and right-click menu. The default event handlers cannot be deleted.
Clone	Select an event handler in this page and click to clone the entry. A cloned entry will have *Copy* added to its name field. You can rename the cloned entry while editing the event handler. This option is available in the toolbar and right-click menu.
Enable	Select to enable the event handler.
Disable	Select to disable the event handler.

Manage event handlers

You can create traffic, event, and extended log handlers to monitor network traffic and events based on specific log filters. These log handlers can then be edited, deleted, cloned, and enabled or disabled as needed.

To create a new event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select *Create New* in the toolbar, or right-click on an the entry and select *Create New* in the right-click menu. The *Create New Event Handler* dialog box is displayed.
3. Enter a name for the new event handler and select *OK*. The *Event Handler* page opens with the *Definition* tab displayed.

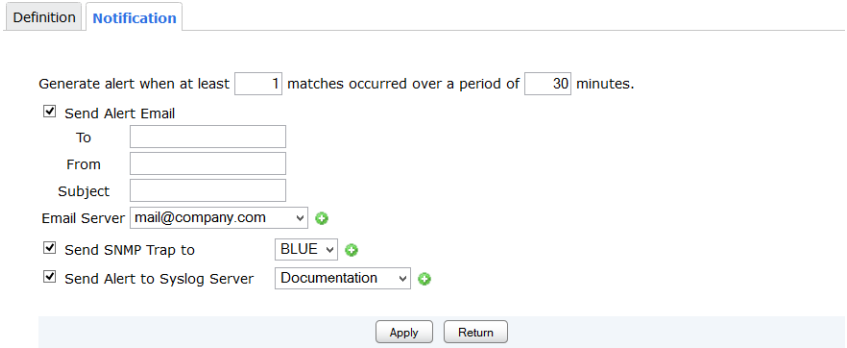


4. Configure the following settings:

Status	Enable or disable the event handler.
Name	Edit the name if required.
Description	Enter a description for the event handler.
Devices	Select *All Devices,* select *Specify* and use the add icon to add devices. Select *Local FortiManager* if the event handler is for local FortiManager event logs. *Local FortiManager* is available in the root ADOM only and is used to query FortiManager event logs.
Severity	Select the severity from the drop-down list, one of: • *Critical* • *High* • *Medium* • *Low*
Filters	
Log Type	Select the log type from the drop-down list. The available options are: *Traffic Log*, *Event Log*, *Application Control*, *DLP*, *IPS*, *Virus*, and *Web Filter*. The *Log Type* is *Event Log* when *Devices* is *Local FortiManager*.
Event Category	Select the category of event that this handler will monitor from the drop-down list. The available options is dependent on the platform type. This option is only available when *Log Type* is set to *Traffic Log* and *Devices* is set to *All Devices* or *Specify*.

Group by	Select the criterium by which the information will be grouped. This option is not available when *Log Type* is set to *Traffic Log*.
Log message that match	Select either *All* or *Any of the Following Conditions*. When *Devices* is *Local FortiManager*, this option is not available.
Add Filter	Select the add icon to add log filters. When *Devices* is *Local FortiManager*, this option is not available. You can only set one log field filter.
Log Field	Select a log field to filter from the drop-down list. The available options will vary depending on the selected log type.
Match Criteria	Select a match criteria from the drop-down list. The available options will vary depending on the selected log field.
Value	Either select a value from the drop-down list, or enter a value in the text box. The available options will vary depending on the selected log field.
Delete	Select the delete icon, to delete the filter. A minimum of one filter is required.
Generic Text Filter	Enter a generic text filter. For more information on creating a text filter, hover the cursor over the help icon.

5. Select *Apply* to save the *Definition* settings.
6. Select the *Notification* tab.



7. Configure the following settings:

Generate alert when at least	Enter threshold values to generate alerts. Enter the number, in the first text box, of each type of event that can occur in the number of minutes entered in the second text box.
Send Alert Email	Select the checkbox to enable. Enter an email address in the *To* and *From* fields, enter a subject in the *Subject* field, and select the email server from the drop-down list. Select the add icon to add an email server.
Send SNMP Trap to	Select the checkbox to enable this feature. Select an SNMP community from the drop-down list. Select the add icon to add a SNMP community.

Send Alert to Syslog Server	Select the checkbox to enable this feature. Select a syslog server from the drop-down list. Select the add icon to add a syslog server.

8. Select *Apply* to create the new event handler.
9. Select *Return* to return to the *Event Handler* page.

To edit an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry and either select *Edit* in the toolbar, or right-click on the entry and select *Edit* in the pop-up menu. The *Edit Event Handler* page opens.
3. Edit the settings as required.
4. Select *Apply* to save the configuration.
5. Select *Return* to return to the *Event Handler* page.

To clone an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry and either select *Clone* in the toolbar, or right-click on the entry and select *Clone* in the pop-up menu. The *Clone Event Handler* window opens.
3. Edit the settings as required.
4. Select *Apply* to save the configuration.
5. Select *Return* to return to the *Event Handler* page.

To delete an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry and either select *Delete* in the toolbar, or right-click on the entry and select *Delete* in the pop-up menu.
3. Select *OK* in the confirmation dialog box to delete the event handler.

The default event handlers cannot be deleted. Use the right-click menu to enable or disable these event handlers. You can also select to clone the default event handlers.

To enable an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry, right-click and select *Enable* in the pop-up menu. The status field will display a enabled icon.

To disable an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry, right-click and select *Disable* in the pop-up menu. The status field will display a disabled icon.

Reports

FortiManager units can analyze information collected from the log files of managed log devices. It then presents the information in tabular and graphical reports that 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, and any other required 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 GUI page to access these options.

The *Reports* tab allows you to configure reports using the predefined report templates, configure report schedules, view report history and the report calendar, and configure and view charts, macros, datasets, and output profiles.

If ADOMs are enabled, each ADOM will have its own report settings including chart library, macro library, dataset library, and output profiles.
FortiCarrier, FortiCache, FortiMail and FortiWeb reports are available when ADOMs are enabled. Reports for these devices are configured within their respective default ADOM. These devices also have device specific charts and datasets.

When rebuilding the SQL database, Reports will not be available until after the rebuild is completed. Select the *Show Progress* link in the message to view the status of the SQL rebuild.

This chapter contains the following sections:

Reports

FortiManager includes preconfigured reports and report templates for FortiGate, FortiMail, and FortiWeb log devices. These report templates can be used as is, or you can clone and edit the templates. You can also create new reports and report templates that can be customized to your requirements.

Predefined report templates are identified by a blue report icon and custom report templates are identified by a green report icon. When a schedule has been enabled, the schedule icon will appear to the left of the report template name.

FortiManager includes preconfigured reports and report templates for FortiGate, FortiMail, and FortiWeb log devices. These report templates can be used as is, or you can clone and edit the templates. You can also create new reports and report templates that can be customized to your requirements.

Predefined report templates are identified by a blue report icon and custom report templates are identified by a green report icon. When a schedule has been enabled, the schedule icon will appear to the left of the report template name.

FortiGate reports

The following tables list the default report templates.

Admin and System Events Report
Application Risk and Control
Application and Risk Analysis
Bandwidth and Applications Report
Client Reputation
Detailed Application Usage and Risk
Email Report
IPS Report
Security Analysis
Threat Report
User Report
User Security Analysis
VPN Report
Web Usage Report
WiFi Network Summary
Wireless PCI Compliance

The following report template can be found in the *Application* folder.

Applications - Top 20 Categories and Applications (Bandwidth)
Applications - Top 20 Categories and Applications (Session)
Applications - Top Allowed and Blocked with Timestamps

The following report templates can be found in the *Detailed User Report* folder.

User Detailed Browsing Log
User Top 500 Websites by Bandwidth
User Top 500 Websites by Session

The following report templates can be found in the *Web* report folder.

Websites - Hourly Website Hits
Websites - Top 20 Category And Websites (Bandwidth)
Websites - Top 20 Category And Websites (Hits)
Websites - Top 500 Sessions by Bandwidth

FortiMail reports

The following table lists report templates exclusive to FortiMail devices.

FortiMail Analysis Report
FortiMail Default Report

FortiWeb report

The following table lists report templates exclusive to FortiWeb devices.

FortiWeb Default Report

FortiCache report

The following table lists report templates exclusive to FortiCache devices.

FortiCache Default Report

Report configuration

In the *Reports* tab, go to *Reports* > *[report]* to view and configure the report configuration, advanced settings, and layout, and to view completed reports. The currently running reports and completed reports are shown in the *View Report* tab, see View report tab on page 394.

Right-clicking on a template in the tree menu opens a pop-up menu with options to *Create New*, *Rename*, *Clone*, *Delete*, *Import*, or *Export* reports, and to *Create New*, *Rename*, or *Delete* folders.

Reports and report templates can be created, edited, cloned, and deleted. You can also import and export report templates. 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:

1. In the *Reports* tab, right-click on *Reports* in the tree menu.
2. Under the *Report* heading, select *Create New*. The *Create New Report* dialog box opens.
3. Enter a name for the new report and select *OK*.
4. Configure report settings in the Configuration tab. The configuration tab includes time period, device selection, report type, schedule, and notifications.

To create a custom cover page, you must select *Print Cover Page* in the *Advanced Settings* menu in the *Advanced Settings* tab.

5. Select the Layout tab to configure the report template.
6. Select the Advanced settings tab to configure report filters and other advanced settings.
7. Select *Apply* to save the report template.

To clone a report:

1. Right-click on the report you would like to clone in the tree menu and select *Clone*. The *Clone Report Template* dialog box opens.
2. Enter a name for the new template, then select *OK*.

   A new template with the same information as the original template is created with the given name. You can then modify the cloned report as required.

To delete a report:

1. Right-click on the report template that you would like to delete in the tree menu, and select *Delete* under the *Report* heading.
2. In the confirmation dialog box, select *OK* to delete the report template.

Import and export

Report templates can be imported from and exported to the management computer.

To import a report template:

1. Right-click on *Reports*, and select *Import*. The *Import Report Template* dialog box opens.
2. Select *Browse*, locate the report template (.dat) file on your management computer, and select *OK*.

The report template will be loaded into the FortiManager unit.

To export a report template:

1. Right-click on the report you would like to export in the tree menu and select *Export*.
2. If a dialog box opens, select to save the file (.dat) to your management computer, and select *OK*.
   The report template can now be imported to another FortiManager device.

Report folders

Report folders can be used to help organize your reports.

To create a new report folder:

1. In the *Reports* tab, right-click on *Reports* in the tree menu. Under the *Folder* heading, select *Create New*.Under the *Folder* heading, select *Create New*.
2. In the *Create New Folder* dialog box, enter a name for the folder, and select *OK*.
   A new folder is created with the given name.

To rename a report folder:

1. Right-click on the report folder that you need to rename in the tree menu.
2. Under the *Folder* heading, select *Rename*.
3. In the *Rename Folder* dialog box, enter a new name for the folder, and select *OK*.

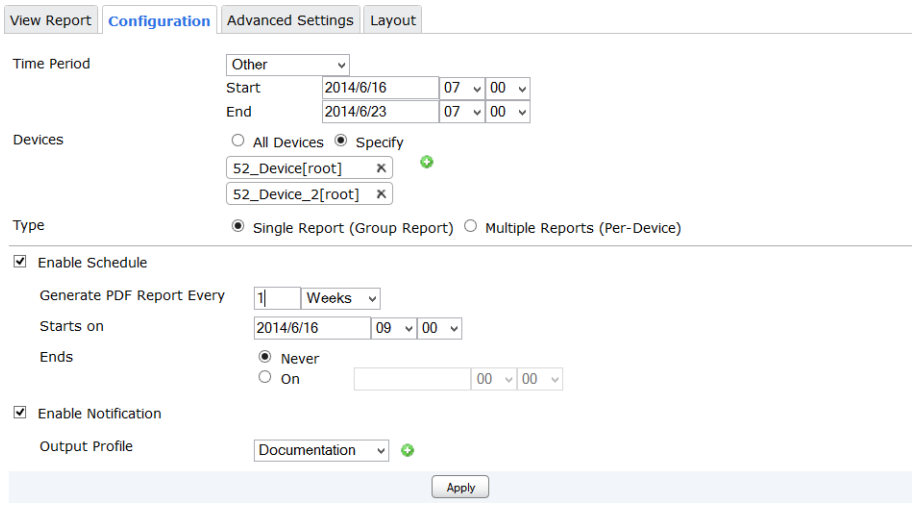
To delete a report folder:

1. Right-click on the report folder that you would like to delete in the tree menu, and select *Delete* under the *Folder* heading.
2. In the confirmation dialog box, select *OK* to delete the report folder.

Configuration tab

In FortiManager v5.2.0 and later, the Reports tab layout has changed. When creating a new report, the *Configuration* tab is the first tab that is displayed. In this tab you can configure the time period, select devices, enable schedules, and enable notification.

Report schedules provide a way to schedule an hourly, daily, weekly, or monthly report so that the report will be generated at a specific time. You can also manually run a report schedule at any time, and enable or disable report schedules. Report schedules can also be edited and disabled from the *Report Calendar*. See Report calendar on page 411 for more information.

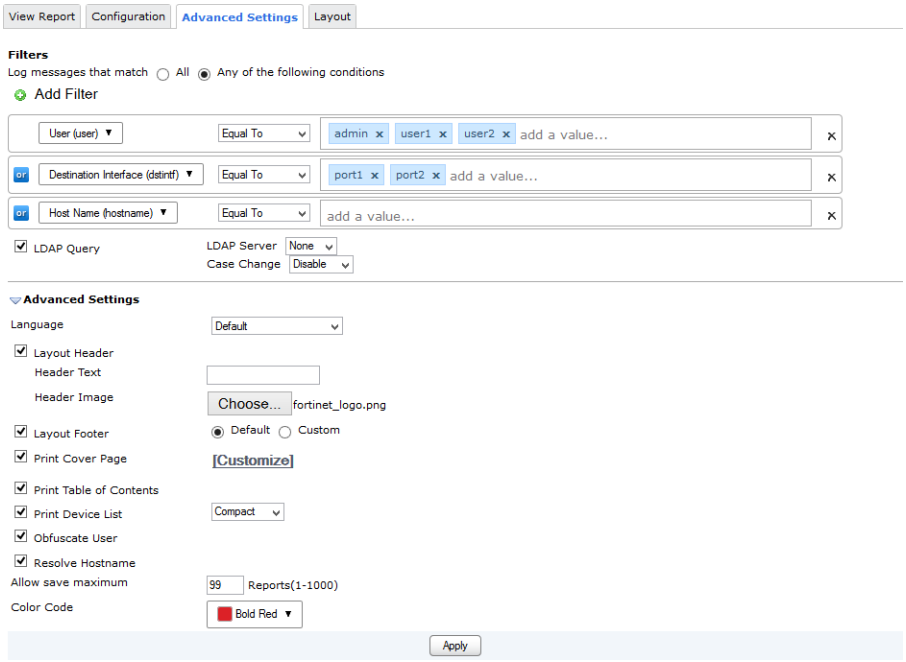


The following settings are available in the *Configuration* tab:

Time Period	The time period that the report will cover. Select a time period, or select *Other* to manually specify the start and end date and time.
Devices	The devices that the report will include. Select either *All Devices or Specify* to add specific devices. Select the add icon to select devices.
User or IP	Enter the user name or the IP address of the user on whom the report will be based.This field is only available for the three predefined report templates in the *Detailed User Report* folder.
Type	Select either *Single Report (Group Report)* or *Multiple Reports (Per-Device)*. This option is only available if multiple devices are selected.
Enable Schedule	Select to enable report template schedules.
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.
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.
Enable Notification	Select to enable report notification.
Output Profile	Select the output profile from the drop-down list, or select *Create New* to create a new output profile. See Output profile on page 416.

Advanced settings tab

After configuring the report configuration, select the *Advanced Settings* tab. In this tab you can configure report filters, LDAP query, and other advanced settings. In the filters section of the *Configuration* tab, you can create and apply log message filters, and add an LDAP query to the report. The *Advanced Settings* section allows you to configure language and print options, and other settings.In this section of the report, you can configure report language, print and customize the cover page, print the table of contents, print a device list, and obfuscate users.



The following settings are available in the *Advanced Settings* tab:

Filters		In the filters section of the *Configuration* tab, you can create and apply log message filters, and add an LDAP query to the report.
	Log messages that match	Select *All* to filter log messages based on all of the added conditions, or select *Any of the following conditions* to filter log messages based on any one of the conditions.
	Add Filter	Select to add filters. For each filter, select the field, and operator from the drop-down lists, then enter or select the values as applicable. Filters vary based on device type.
	LDAP Query	Select to add an LDAP query, then select the LDAP server and the case change value from the drop-down lists.
Advanced Settings		Configure advanced report settings.

	Language	Select the report language. Select one of the following: *Default, English*, *French*, *Japanese*, *Korean*, *Portuguese*, *Simplified_Chinese*, *Spanish*, or *Traditional_Chinese*.
	Layout Header	Enter header text and select the header image. The default image is *fortinet_logo.png*.
	Layout Footer	Select either a default footer or custom footer. When selecting *Custom*, enter the footer text in the text field.
	Print Cover Page	Select to print the report cover page. Select *Customize* to customize the cover page.
	Print Table of Contents	Select to include a table of contents.
	Print Device List	Select to print the device list. Select *Compact*, *Count*, or *Detailed* from the drop-down list.
	Print Report Filters	Select to print the filters applied to the report.
	Obfuscate User	Select to hide user information in the report.
	Resolve Hostname	Select to resolve hostnames in the report. The default status is enabled.
	Allow save maximum	Select a value between 1-1000 for the maximum number of reports to save.
	Color Code	The color used to identify the report on the calendar. Select a color code from the drop-down list to apply to the report schedule. Color options include: *Bold Blue*, *Blue*, *Turquoise*, *Green*, *Bold Green*, *Yellow*, *Orange*, *Red*, *Bold Red*, *Purple*, and *Gray*.

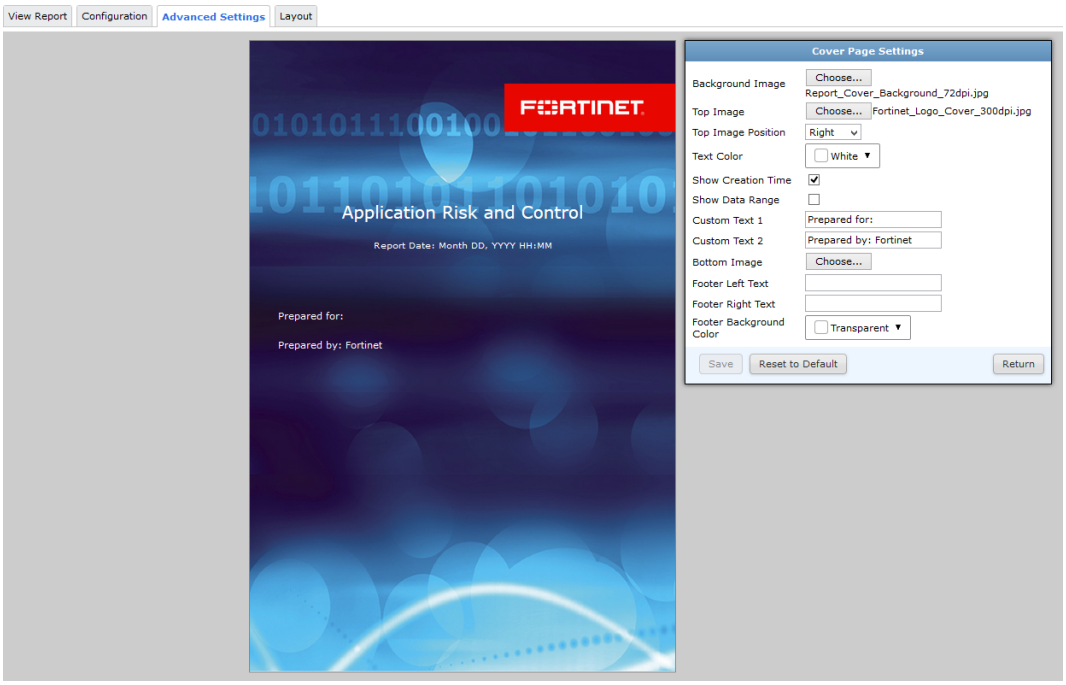
Report cover pages

The report cover page is only included in the report when enabled in the *Advanced Settings* menu in the *Advanced Settings* tab. See Advanced settings tab on page 391.

When enabled, the cover page can be edited to contain the desired information and imagery.

To edit cover page settings:

1. In the *Reports* tab, select the report in the tree menu whose cover page you are editing, then select the *Advanced Settings* tab.
2. In the *Advanced Settings* section, select *Customize* next to the *Print Cover Page* option. The *Cover Page Settings* page opens.



3. Configure the following settings:

Background Image	Select *Choose* to open the *Choose a graphic* dialog box. Select an image, or select *Upload* to find an image on the management computer, then select *OK* to add the image as the background image of the cover page.
Top Image	Select *Choose* to open the *Choose a graphic* dialog box. Select an image, or select *Upload* to find an image on the management computer, then select *OK* to add the image at the top of the cover page.
Top Image Position	Select the top image position from the drop-down menu. Select one of the following: Right, Center, Left.
Text Color	Select the text color from the drop-down menu. Select one of the following: Black, Bold Blue, Blue, Turquoise, Green, Bold Green, Yellow, Orange, Red, Bold Red, Purple, While, Gray.
Show Creation Time	Select to print the report date on the cover page.
Show Data Range	Select to print the data range on the cover page.
Custom Text 1	Enter custom text for the *Custom Text 1* field.
Custom Text 2	Enter custom text for the *Custom Text 2* field.
Bottom Image	Select *Choose* to open the *Choose a graphic* dialog box. Select an image, or select *Upload* to find an image on the management computer, then select *OK* to add the image at the bottom of the cover page.

Footer Left Text	Edit the text printed in the left hand footer of the cover page.
Footer Right Text	Edit the text printed in the left hand footer of the cover page. `{default}` prints the report creation date and time.
Footer Background Color	Select the cover page footer background color from the drop-down list. Select one of the following: Black, Bold Blue, Blue, Turquoise, Green, Bold Green, Yellow, Orange, Red, Bold Red, Purple, While, Gray, Transparent.
Reset to Default	Select to reset the cover page settings to their default settings.

4. Select *Save* in the toolbar, to save your changes.
5. Select *Return* in the toolbar, to return to *Advanced Settings* tab.

View report tab

A report can be manually run at any time by selecting *Run Report Now*.

Competed reports are displayed in the *View Report* tab of the *Reports* tab. The report name, available formats, and completion time or status are shown in the table. Reports can be viewed in HTML or as PDFs.

The toolbar and the right-click menu provide options to delete or download the selected reports, as well as to run the report.

Completed reports can be viewed for specific devices from the *Device Manager* tab.

Completed reports can also be downloaded and deleted from the *Report Calendar* page. See Report calendar on page 411.

The following options are available:

Report Name	The name of the report. Click the column header to sort entries in the table by report name.
Format	Select *HTML* to open the report in HTML format in a new web browser tab or window, depending on your browser settings. Select *PDF* to open or download the report in PDF format.
Completion Time/Status	The completion status of the report, or, if the report is complete, the data, and time (including time zone) that the report completed. Click the column header to sort entries in the table by completion time.

Right-click on an report in the list to open the right-click menu. The following options are available:

Run Report Now	Select to run the report now.
Delete	Select one or more reports in the completed reports list, then select *Delete* from the toolbar or right-click menu. Select *OK* in the confirmation dialog box to delete the selected report or reports.

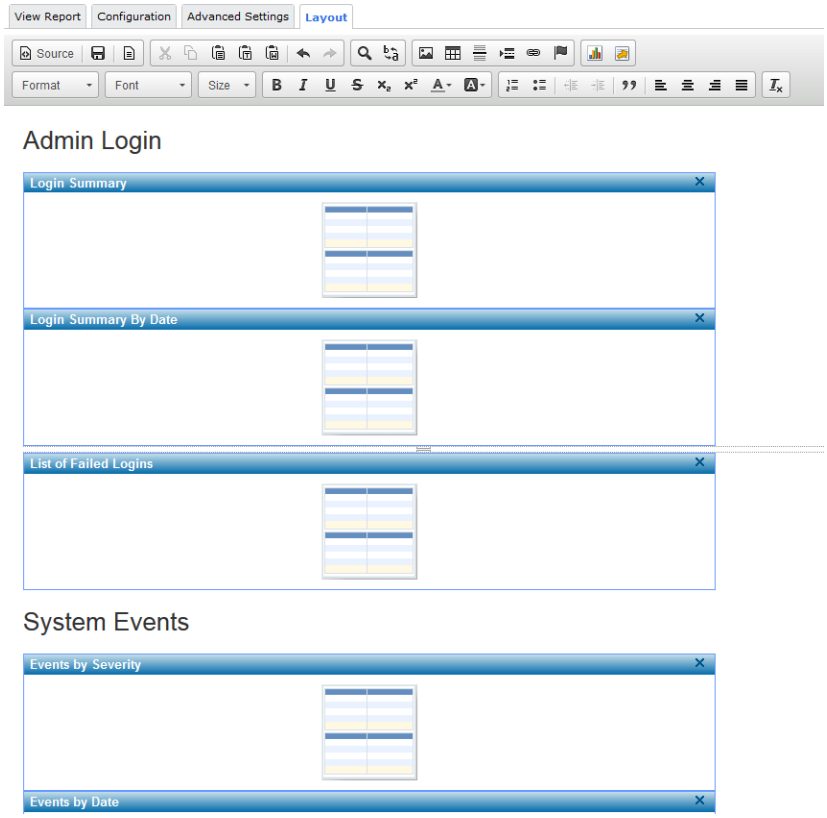
Download	Select one reports in the completed reports list, then select *Download* from the toolbar or right-click menu to download the selected report or reports. Each report will be saved individually as a PDF file on the management computer. Reports that are not done cannot be downloaded.

To view device reports:

1. In the *Device Manager* tab, select the ADOM that contains the device whose report you would like to view, and select the device. You can select to view reports by device or by VDOM. All of the reports that have been run for the selected device are shown in the left content pane.
2. Select a format from the *Format* column to open the report in that format in a new browser window or tab.
3. Select a report, then select *Download* from the right-click menu to download the selected report.
4. Select one or more reports, then select *Delete* to delete the selected reports.

Report layouts

In the *Layout* tab, you can configure report template layout. Various content can be added to a report template, such as charts, images, and typographic elements, using the layout toolbar. The template color scheme, fonts, and layout can be controlled, and all the report elements can be edited and customized as needed.



Because the cut, copy and paste functions need access to the clipboard of your operating system, some Internet browsers either block it when called from layout editor toolbar, or ask you to explicitly agree to that. Should accessing the clipboard by clicking the respective cut, copy and paste buttons from toolbar or context menu options be blocked, you can always perform these operations with keyboard shortcuts.

The following options are available in the layout editor:

Source	Select to view and configure the report layout in XML format.
Save	Select to save changes to the report layout.
Templates	Select to choose the template to open in the editor. Select one of the following: • Image and Title: One main image with a title and text that surround the image. • Strange Template: A template that defines two columns, each one with a different title, and some text. • Text and Table: A title with some text and a table. You can select to replace actual contents.
Cut	To cut a text fragment, start with selecting it. When the text is selected, you can cut it using one of the following methods: • Select the cut button in the toolbar • Right-click and select cut in the menu • Use the *Ctrl+X* shortcut on your keyboard.
Copy	To cut a text fragment, start with selecting it. When the text is selected, you can cut it using one of the following methods: • Select the cut button in the toolbar • Right-click and select cut in the menu • Use the *Ctrl+C* shortcut on your keyboard.
Paste	To paste a text fragment, start with cutting it or copying from another source. Depending on the security settings of your browser, you may either paste directly from the clipboard or use *Paste* dialog window.
Paste as plain text	If you want to paste an already formatted text, but without preserving the formatting, you can paste it as plain text. To achieve this, copy the formatted text and select the *Paste as plain text* button in the toolbar. If the browser blocks the editor toolbar's access to clipboard, a *Paste as Plain Text* dialog window will appear and you will be asked to paste the fragment into the text box using the *Ctrl+V* keyboard shortcut.

Paste from Word	You can preserve basic formatting when you paste a text fragment from Microsoft Word. To achieve this, copy the text in a Word document and paste it using one of the following methods: • Select the Paste from Word button in the toolbar • Use the *Ctrl+V* shortcut on your keyboard.
Undo	Select to undo the last action. Alternatively, use the *Ctrl+Z* keyboard shortcut to perform the undo operation.
Redo	Select to redo the last action. Alternatively, use the *Ctrl+Y* keyboard shortcut to perform the redo operation.
Find	Select to find text in the report layout editor. Find consists of the following elements: • Find what: Is the text field where you enter the word or phrase that you want to find. • Match case: Checking this option limits the search operation to words whose case matches the spelling (uppercase and lowercase letters) given in the search field. This means that the search becomes case-sensitive. • Match whole word: Checking this option limits the search operation to whole words. • Match cyclic: Checking this option means that after editor reaches the end of the document, the search continues from the beginning of the text. This option is checked by default.
Replace	Select to replace text in the report layout editor. Replace consists of the following elements: • Find what: Is the text field where you enter the word or phrase that you want to find. • Replace with: Is the text field where you enter the word or phrase that will replace the search term in the document. • Match case: Checking this option limits the search operation to words whose case matches the spelling (uppercase and lowercase letters) given in the search field. This means that the search becomes case-sensitive. • Match whole word: Checking this option limits the search operation to whole words. • Match cyclic: Checking this option means that after editor reaches the end of the document, the search continues from the beginning of the text. This option is checked by default.
Image	Select the *Image* button in the toolbar to insert an image into the report layout. Right-click an existing image to edit image properties.

Table	Select the *Table* button in the toolbar to insert a table into the report layout. Right-click an existing table to edit a cell, row, column, table properties or delete the table.
Insert Horizontal Line	Select to insert a horizontal line.
Insert Page Break for Printing	Select to insert a page break for printing.
Link	Select the *Link* button in the toolbar to open the *Link* dialog window. You can select to insert a URL, a link to an anchor in the text, or an email address. Alternatively, use the *Ctrl+L* keyboard shortcut to open the *Link* dialog window. See Link on page 402 for more information.
Anchor	Select the *Anchor* button in the toolbar to insert an anchor in the report layout.
FortiAnalyzer Chart	Select to insert a FortiAnalyzer chart. See Charts on page 402 for more information.
FortiAnalyzer Macro	Select to insert a FortiAnalyzer macro. See Macros on page 403 for more information.
Paragraph Format	Select the paragraph format from the drop-down list. Select one of the following: Normal, Heading 1, Heading 2, Heading 3, Heading 4, Heading 5, Heading 6, Formatted, or Address.
Font Name	Select the font from the drop-down list. Select one of the following: Arial, Comic Sans MS, Courier New, Georgia, Lucida Sans Unicode, Tahoma, Times New Roman, Trebuchet MS, or Verdana.
Font Size	Select the font size from the drop-down list. Select a size ranging from 8 to 72.
Bold	Select the text fragment and then select the *Bold* button in the toolbar. Alternatively, use the *Ctrl+B* keyboard shortcut to apply bold formatting to a text fragment.
Italic	Select the text fragment and then select the *Italic* button in the toolbar. Alternatively, use the *Ctrl+I* keyboard shortcut to apply italics formatting to a text fragment.
Underline	Select the text fragment and then select the *Underline* button in the toolbar. Alternatively, use the *Ctrl+U* keyboard shortcut to apply underline formatting to a text fragment.
Strike Through	Select the text fragment and then select the *Strike Through* button in the toolbar.

Subscript	Select the text fragment and then select the *Subscript* button in the toolbar.
Superscript	Select the text fragment and then select the *Superscript* button in the toolbar.
Text Color	You can change the color of text in the report by using a color palette. To choose a color, select a text fragment and press the *Text Color* toolbar button. The *Text Color* drop-down menu that will open lets you select a color from a basic palette of 40 shades. If the color that you are after is not included in the basic palette, click the *More Colors* option in the drop-down menu. The *Select Color* dialog window that will open lets you choose a color from an extended palette.
Background Color	You can also change the color of the text background.
Insert/Remove Numbered List	Select to insert or remove a numbered list.
Insert/Remove Bulleted List	Select to insert or remove a bulleted list.
Decrease Indent	To decrease the indentation of the element, select the *Decrease Indent* toolbar button. The indentation of a block-level element containing the cursor will decrease by one tabulator length.
Increase Indent	To increase the indentation of the element, select the *Increase Indent* toolbar button. The block-level element containing the cursor will be indented with one tabulator length.
Block Quote	Block quote is used for longer quotations that are distinguished from the main text by left and right indentation. It is recommended to use this type of formatting when the quoted text consists of several lines or at least 100 words.
Align Left	When you align your text left, the paragraph is aligned with the left margin and the text is ragged on the right side. This is usually the default text alignment setting for the languages with left to right direction.
Center	When you center your text, the paragraph is aligned symmetrically along the vertical axis and the text is ragged on the both sides. This setting is often used in titles or table cells.
Align Right	When you align your text right, the paragraph is aligned with the right margin and the text is ragged on the left side. This is usually the default text alignment setting for the languages with right to left direction.
Justify	When you justify your text, the paragraph is aligned with both left and right margin; the text is not ragged on any side. Instead of this, additional spacing is realized through flexible amount of space between letters and words that can stretch or contract according to the needs.

Remove Format	Select to remove formatting.

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

Cut	Select text or a report element, right-click and select cut in the menu.
Copy	Select text or a report element, right-click and select copy in the menu.
Paste	Select a location in the report layout, right-click and select paste in the menu.
Cell	Right-click a table in the layout and select to edit cell settings including: inserting cells, deleting cells, merge, split, and cell properties.
Row	Right-click a table in the layout and select to edit row settings including: inserting rows and deleting rows.
Column	Right-click a table in the layout and select to edit column settings including: inserting columns and deleting columns.
Delete Table	Right-click a table in the layout and select to delete the table.
Chart Properties	Right-click a chart in the layout to edit the chart properties including: chart selection, title, width, and filters.
Table Properties	Right-click a table in the layout to edit the table properties including the following: rows, width, columns, height, headers, cell spacing, border size, cell pading, alignment, caption, and summary.
Image Properties	Right-click an image in the layout to edit the image properties including: image selection, width, height, lock ratio, reset size, and alternative text.
Macro Properties	Right-click a macro in the layout to edit the macro.
Edit Link	Right-click a link in the layout to edit the link properties including: link type, protocol, and URL.
Unlink	Right-click a link in the layout and select to remove the link.
Edit Anchor	Right-click an anchor in the layout and select to edit anchor properties.
Remove Anchor	Right-click an anchor in the layout and select to remove the anchor.

Inserting images

To insert an image in the report layout, select the *Image* button in the toolbar. The *Image Properties* dialog window opens and you can set configuration options that define image source, its size, display properties, and other advanced properties.

The following options are available:

Browse	Select and browse to the image you want to insert into the report layout.
Width	Enter the width of the image in pixels.
Height	Enter the height of the image in pixels.
Lock Ratio	Select to lock the ratio.
Reset Size	Select to reset the size.
Alternative Text	Enter a short textual description of the image that tells users with assistive devices (like screen readers) what the image is about.

Creating a table

To create a table in the report layout, select the *Table* button in the toolbar. The *Table Properties* dialog window opens and you can set configuration options that define table size, its display properties, and other advanced properties.

The following options are available:

Rows	Enter the number of rows in the table.
Width	Enter the width of the table in pixels or a percent value
Columns	Enter the number of columns in the table.
Height	Enter the height of the table in pixels.
Headers	Select the header from the drop-down list. Select one of: None, First Row, First Column, Both.
Cell spacing	Enter a value for the space between individual cells as well as cells and table borders, in pixels.
Border size	Enter a value for the thickness of the table border in pixels.
Cell padding	Enter a value for the space between the cell border and its contents, in pixels.
Alignment	Select the alignment from the drop-down list. Select one of: Left, Center, Right.
Caption	Enter the label of the table that will displayed at the top of the table.
Summary	Enter a short textual summary of the table that tells users with assistive devices (like screen readers) what the table is about.

Link

Select the *Link* button in the toolbar to open the *Link* dialog window. You can select to insert a URL, a link to an anchor in the text, or an email address.

The following options are available:

Link Type	Select the link type from the drop-down list. Select one of: URL, Link to anchor in text, E-mail.
URL	Select the protocol (http://, https://, ftp://, news://, <other>) and enter the URL in text field.
Link to anchor in text	Select an anchor by anchor name or by element ID.
E-mail	Enter the email address, message subject, and message body.

Anchor

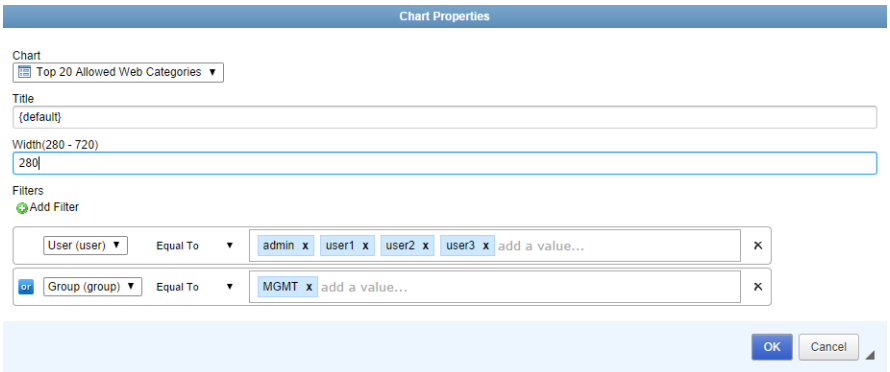
1. Select the *Anchor* button in the toolbar. The *Anchor Properties* dialog windows will appear. Enter an anchor name in the text field. Once you select *OK*, an anchor icon will appear in the report layout. You can then create a link to the anchor by select the *Link* button.
2. Right-click an anchor to edit or delete the anchor.

Charts

Chart elements can be placed in the report template. The chart content can be filtered, and the chart content can be edited.

To add a chart:

1. Click the FortiAnalyzer chart icon. The *Chart Properties* dialog box will open.



2. The following options are available:

Chart	Select the chart from the drop-down list. Search for the chart by entering all or part of the chart name into the *Search* field.

Title	Optionally, change the chart title.
Width	Select the chart width. Type a value between 280 and 720.
Filters	Select to add filters. For each filter, select the field, and operator from the drop-down lists, then enter or select the values as applicable. Filters vary based on device type.

3. Select *OK* once you have found and selected the chart you would like to add.
   The chart's placeholder will appear. You can drag-and-drop the chart to a new location in the report layout.

To add additional chart filters:

1. Select the chart, right-click, and select *Chart Properties* in the menu. Alternatively, double-click on the chart. The *Chart Properties* dialog box will open.
2. Add charts filters to the chart as needed.
3. Select *OK* to apply the filters to the chart and return to the report layout page.

To edit a chart:

1. Select the chart, right-click, and select *Chart Properties* in the menu. Alternatively, double-click on the chart. The *Chart Properties* dialog box will open.
2. Edit the chart as needed.
3. Select *OK* to apply your changes.

Macros

FortiManagermacro elements can be added to the report template. Select the Macro button in the toolbar and select the macro from the drop-down list. Right-click an existing macro to open macro properties.

Chart library

The FortiManager unit provides a selection of predefined charts. New charts can be created using the custom chart wizard, by cloning and editing an existing chart, or by using the advanced chart creation option. You can select to display predefined chart, custom charts, or both.

To view a listing of the available predefined charts, see Appendix E - Charts, Datasets, & Macros on page 446.

For advanced users, right-click the right content pane and select *Create New* to create SQL based charts. See Managing charts on page 406.

Charts are predefined to show specific information in an appropriate format, such as pie charts or tables. They are organized into categories, and can be added to, removed from, and organized in reports.

To view the chart library, go to *Reports* > *Chart Library*.

The following information is displayed:

Name	The name of the chart. Click the column header to sort entries in the table by name.
Description	The chart description. Click the column header to sort entries in the table by description.
Category	The chart category. Click the column header to sort entries in the table by category.
Search	Enter a search term in the search field to find a specific chart.
Pagination	Adjust the number of entries that are listed per page and browse through the pages.

The following options are available in the toolbar:

Wizard	Launch the custom chart wizard. This option is only available for FortiGate and FortiCarrier ADOMs.
Create New	Create a new chart. For FortiGate and FortiCarrier ADOMs, this option is only available from the right-click menu.
Edit	Select to edit a chart. This option is only available for custom charts.
View	Select to view chart details. This option is only available for predefined charts, as they cannot be edited.
Delete	Select to delete a chart. This option is only available for custom charts.
Clone	Select to clone an existing chart.
Show Predefined	Select to display predefined charts.
Show Custom	Select to display custom charts.

Custom chart wizard

The custom chart wizard is a step by step guide to help you create custom charts. It is only available for FortiGate and FortiCarrier ADOMs.

To start the custom chart wizard, go to *Reports* > *Chart Library*, and select *Wizard* in the toolbar. Follow the steps in the chart wizard, outlined below, to create a custom chart.

Select the *Tutorial* icon on any of the wizard windows to view the online chart wizard video.

Step 1 of 3 - Choose data

Configure the data that the custom chart will use, then select Next to proceed to the next step:

Log Type	Select either *Traffic Log* or *Event Log*.
Group by	Select how the data are grouped. Depending on the chart type selected in step 3, this selection will relate to *Column 1* (Table), the *Y-axis* (Bar and Line graphs), or the *Legend* (Pie chart). The available options will vary depending on the selected log type: • Traffic log: *Application Category, Application ID, Application Name, Attack, Destination Country, Destination Interface, Destination IP, Device Type, Source Interface, Source IP, Source SSID, User, Virus, VPN, VPN Type, Web Category*, or *Website (Hostname)*. • Event log: *VPN Tunnel*, or *Remote IP*.
Aggregate by	Select how the data is aggregated. Depending on the chart type selected in step 3, this selection will relate to *Column 2* (Table), the *X-axis* (Bar and Line graphs), or the *Value* (Pie chart). The following options are available: *Duration*, *Received Bytes*, *Sent Bytes*, *Total Bytes*, *Total Sessions* or *Total Blocked Sessions* (Traffic log only).
Show	Select how much data to show in the chart from the drop-down list. One of the following: *Top 5*, *Top 10*, *Top 25*, *Top 50*, or *Top 100*.

Step 2 of 3 - Add filters

You can add one or more filters to the chart. These filters will be permanently saved to the dataset query.

Match	Select *All* to filter data based on all of the added conditions, or select *Any of the Following Conditions* to filter the data based on any one of the conditions.
Add	Select to add filters. For each filter, select the field, and operator from the drop-down lists, then enter or select the value as applicable. Filters vary based on device type. The available filters vary depending on the log type selected. Select the delete icon to remove a filter.
Destination Interface	This filter is available for traffic logs only. The available operators are: *Equals*, *Not Equal*, *Contains*, and *Not Contain*.
Destination IP	This filter is available for traffic logs only. The available operators are: *Equals*, *Not Equal*, and *Range*. If *Range* is selected, enter the starting and ending IP address in the value fields.
Security Action	This filter is available for traffic logs only. The available operators are: *Equals* and *Not Equal*. The value is always *Pass Through*.

Security Event	Select *Equals or Not Equal* from the second drop-down list. Select one of the below options from the third drop-down list.This filter is available for traffic logs only. The value can be one of the following: *Analytics*, *Application Control*, *AV Error*, *Banned Word*, *Command Block*, *DLP*, *File Filter*, *General Mail Log*, *HTML Script Virus*, *IPS*, *MIME Fragmented*, *MMS Checksum*, *MMS Dupe*, *MMS Endpoint*, *MMS Flood*, *MAC Quarantine*, *Oversize*, *Script Filter*, *Spam Filter*, *SSH Block*, *SSH Log*, *Switching Protocols*, *Virus*, *VOIP*, *Web Content*, *Web Filter*, or *Worm*.
Service	This filter is available for both traffic and event logs. The available operators are: *Equals*, *Not Equal*, *Contains*, and *Not Contain*.
Source Interface	This filter is available for traffic logs only. The available operators are: *Equals*, *Not Equal*, *Contains*, and *Not Contain*.
Source IP	This filter is available for traffic logs only. The available operators are: *Equals*, *Not Equal*, and *Range*. If *Range* is selected, enter the starting and ending IP address in the value fields.
User	This filter is available for both traffic and event logs. The available operators are: *Equals*, *Not Equal*, *Contains*, and *Not Contain*.

Step 3 of 3 - Preview

The preview page allows you to select the chart type and rename the custom chart.

Chart Type	Select the chart type in the drop-down list; one of the following: *Bar*, *Line*, *Pie*, or *Table*. Depending on the chart settings configured in the previous two steps, the available options may be limited.
Column 1 / Y-axis / Legend	Displays the *Group by* selection. The field varies depending on the chart type.
Column 2 / X-axis / Value	Displays the *Aggregate by* selection. The field varies depending on the chart type.
Name	Displays the default name of the custom chart. This field can be edited.

Select *Finish* to finish the wizard and create the custom chart. The custom chart will be added to the chart table and will be available for use in report templates.

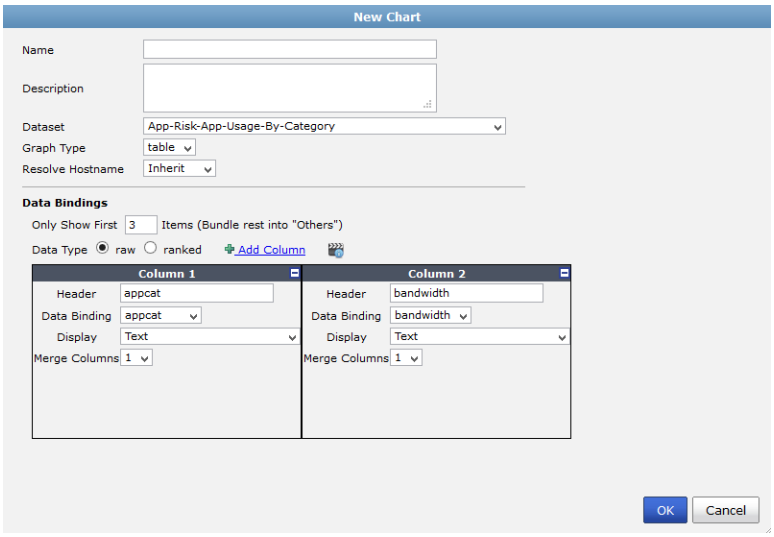
Managing charts

Predefined charts can be viewed and cloned. Custom charts can be created, edited, cloned, and deleted.

To create a new chart:

1. In the chart library:
   - If you are creating a chart in a FortiGate or FortiCarrier ADOM: right-click in the content pane and select *Create New*.
   - If you are creating a chart in any other ADOM: select *Create New* in the toolbar.

   The *New Chart* dialog box opens.



2. Select the *Tutorial* icon to view the online chart creation video.
3. Enter the required information for the new chart.

Name	Enter a name for the chart.
Description	Enter a description of the chart.
Dataset	Select a dataset from the drop-down list. See Dataset on page 413 for more information. The options will vary based on device type.
Graph Type	Select a graph type from the drop-down list; one of: *table*, *bar*, *pie*, or *line*. This selection will affect the rest of the available selections.
Line Subtype	Select one of the following options: *basic*, *stacked*, or *back-to-back*. This option is only available when creating a line graph.
Resolve Hostname	Select to resolve the hostname. Select one of the following: *Inherit*, *Enabled*, or *Disabled*.
Data Bindings	The data bindings vary depending on the chart type selected.
bar, pie, or line graphs	

X-Axis	*Data Binding*: Select a value from the drop-down list. The available options will vary depending on the selected dataset. *Only Show First*: Enter a numerical value. Only the first 'X' items will be displayed. Other items are bundled into the *Others* category. *Overwrite label*: Enter a label for the axis.
Y-axis	*Data Binding*: Select a value from the drop-down list. The available options will vary depending on the selected dataset. *Overwrite label*: Enter a label for the axis. *Group by:* Select a value from the drop-down list. The available options will vary depending on the selected dataset. This option is only available when creating a bar graph.
Order By	Select to order by the X-Axis or Y-Axis. This option is only available when creating a line or bar graph.
table	
Only Show First Items	Enter a numerical value. Only the first 'X' items will be displayed. Other items are bundled into the Others category. This option is available for all columns when Data Type is set to raw. When Data Type is set to ranked, this option is available in Column 1.
Data Type	Select either *ranked* or *raw*.
Add Column	Select add column icon to add a column.
Columns	Up to fifteen columns can be added. The following column settings must be set: • *Header*: Enter header information. • *Data Binding*: Select a value from the drop-down list. The options vary depending on the selected dataset. • *Display*: Select a value from the drop-down list. • *Merge Columns*: Select a value from the drop-down list. This option is only available when *Data Type* is *raw*. If applicable, enter a *Merge Header*. • *Order by this column*: Select to order the table by this column. This option is only available in *Column 1* when *Data Type* is *ranked*.

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

To clone a chart:

1. In the chart library, select the chart that you would like to clone and select *Clone* from either the toolbar or right-click menu. The *Clone Chart* dialog box opens.
2. Edit the information as needed, then select *OK* to clone the chart.

To edit a chart:

1. In the chart library, double-click on the custom chart you need to edit, or select the chart then select *Edit* from either the toolbar or right-click menu. The *Edit Chart* dialog box opens.
2. Edit the information as required, then select *OK* to finish editing the chart.

Predefined charts cannot be edited, the information is read-only. A predefined chart can be cloned, and changes can then be made to said clone.

To delete charts:

1. In the chart library, select the custom chart or charts that you would like to delete and select *Delete* from either the toolbar or right-click menu.
2. Select *OK* in the confirmation dialog box to delete the chart or charts.

Predefined charts cannot be deleted.

Macro library

The FortiManager unit provides a selection of predefined macros. You can create new macros and clone existing macros. You can select to display predefined macros, custom macros, or both.

To view a listing of the available predefined macros, see Appendix E - Charts, Datasets, & Macros.

Macros are predefined to use specific datasets and queries. They are organized into categories, and can be added to, removed from, and organized in reports.

Macros are currently supported in FortiGate and FortiCarrier ADOMs only.

To view the macro library, go to *Reports* > *Macro Library*.

The following information is available:

Name	The name of the macro.
Description	The macro description.
Category	The macro category.
Pagination	Adjust the number of entries that are listed per page and browse through the pages.

The following options are available in the toolbar:

Create New	Create a new macro. This option is only available from the right-click menu.
Edit	Select to edit a macro. This option is only available for custom macros.
View	Select to view macro details. This option is only available for predefined macros, as they cannot be edited.

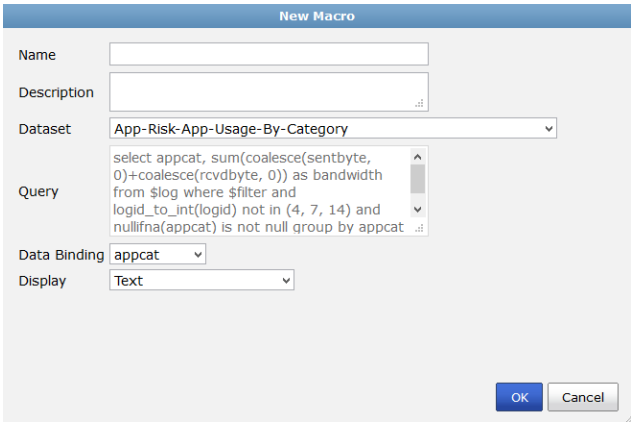
Delete	Select to delete a macro. This option is only available for custom macros.
Clone	Select to clone an existing macro.
Show Predefined	Select to display predefined macros.
Show Custom	Select to display custom macros.
Search	Enter a search term in the search field to find a specific macros.

Managing macros

Predefined macros can be viewed and cloned. Custom macros can be created, edited, cloned, and deleted. You can insert macros into text elements in the report layout.

To create a new macro:

1. In the macro library, select *Create New* in the toolbar or right-click in the content pane and select *Create New*. The *New Macro* dialog box opens.



2. Enter the required information for the new macro.

Name	Enter a name for the macro.
Description	Enter a description of the macro.
Dataset	Select a dataset from the drop-down list.The options will vary based on device type.
Query	Displays the query statement for the dataset selected.
Data Binding	The data bindings vary depending on the dataset selected. Select a data binding from the drop-down list.
Display	Select a value from the drop-down list.

3. Select *OK* to create the new macro.

To clone a macro:

1. In the macro library, select the macro that you would like to clone and select *Clone* from either the toolbar or right-click menu. The *Clone Macro* dialog box opens.
2. Edit the information as needed, then select *OK* to clone the macro.

To view a predefined macro:

1. In the macro library, double-click on the predefined macro you would like to view, or select the macro then select *View* from either the toolbar or right-click menu. The *View Macro* dialog box opens. All fields are read-only.
2. Select *Close* when you are finished.

To edit a macro:

1. In the macro library, double-click on the custom macro you need to edit, or select the macro then select *Edit* from either the toolbar or right-click menu. The *Edit Macro* dialog box opens.
2. Edit the information as required, then select *OK* to finish editing the macro.

To delete macros:

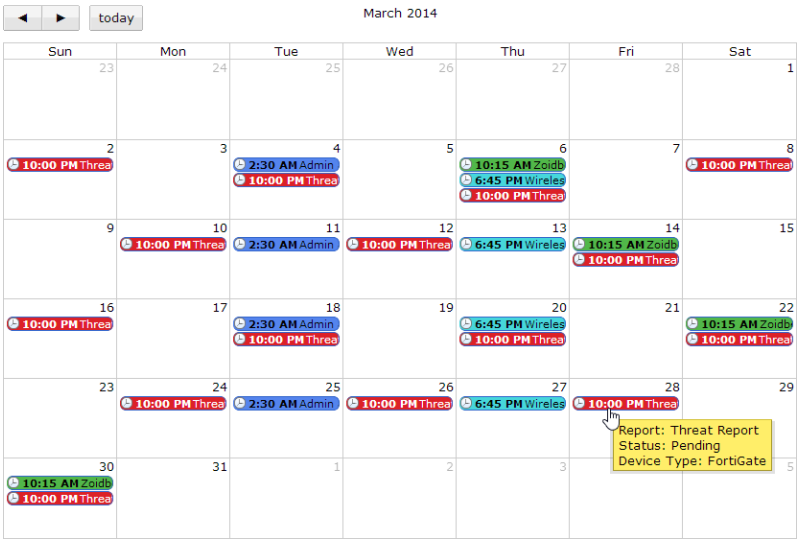
1. In the macro library, select the custom macro or macros that you would like to delete and select *Delete* from either the toolbar or right-click menu.
2. Select *OK* in the confirmation dialog box to delete the macro or macros.

Predefined macros cannot be deleted.

Report calendar

The report calendar provides an overview of scheduled reports. You can view all reports scheduled for the selected month. From the calendar page, you can edit and disable upcoming reports, and delete or download completed reports.

To view the report calendar, go to *Reports* > *Report Calendar*.



Hovering the mouse cursor over a scheduled report on the calendar opens a notification box that shows the report's name and status, as well as the device type.

Selecting the left and right arrows at the top of the calendar page will adjust the month that is shown. Select *Today* to return to the current month.

To edit a report schedule:

1. Right-click on the scheduled report in the report calendar and select *Edit*. The *Edit Report* window will open.
2. Edit the report settings as required, then select *Apply* to apply the changes.

To disable a scheduled report:

1. Right-click the scheduled report and select *Disable* from the right-click menu.
2. In the confirmation box, select *OK*.

   Disabling a report will remove all scheduled instances of the report from the report calendar. Completed reports will remain in the report calendar.

To delete a scheduled report:

1. Right-click the scheduled report that you would like to delete and select *Delete*. Only scheduled reports that have already been run can be deleted.
2. Select *OK* in the confirmation dialog box to delete the scheduled report.

To download a report:

1. Right-click the scheduled report that you would like to download and select *Download*. Only scheduled reports that have already been run can be downloaded.
2. Depending on your web browser and management computer settings, save the file to your computer, or open the file in an applicable program.

   Reports are downloaded as PDF files.

Advanced

The advanced menu allows you to view, configure and test datasets, create output profiles, and manage report languages.

Dataset

FortiManager datasets are collections of log files from monitored devices. Reports are generated based on these datasets.

To view a listing of the available predefined datasets, see Appendix E - Charts, Datasets, & Macros.

Predefined datasets for each supported device type are provided, and new datasets can be created and configured. Both predefined and custom datasets can be cloned, but only custom datasets can be deleted. You can also view the SQL query for a dataset, and test the query against specific devices or all devices.

To view and configure datasets, go to *Reports* > *Advanced* > *Dataset* in the tree menu.

The following information is displayed:

Name	The name of the dataset.
Device Type	The device type that the dataset applies to.
Log Type	The type of log that the dataset applies to.
Pagination	Adjust the number of logs that are listed per page and browse through the pages.

The following options are available in the toolbar:

Create New	Select to create a new dataset.
View	Select to view the dataset. View is only available for pre-defined datasets.
Edit	Select to edit an existing dataset.
Delete	Select to delete a dataset.
Clone	Select to clone an existing dataset.
Search	Use the search field to find a specific dataset.

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

Create New	Select to create a new dataset.

View	Select a dataset, right-click, and select *View* to view the dataset selected. View is only available for pre-defined datasets.
Delete	Select a custom dataset, right-click, and select *Delete* to remove the custom dataset. You cannot delete pre-defined datasets.
Clone	Select a custom dataset, right-click, and select *Clone* to clone the dataset.
Validate	Select a custom dataset, right-click, and select *Validate* to validate the selected dataset. A validation result dialog box will be displayed with the results.
Validate All Custom	Right-click in the right pane and select *Validate All Custom* to validate all custom datasets. A validation result dialog box will be displayed with the results.

To create a new dataset:

1. In the dataset list, either select *Create New* from the toolbar, or right-click in the dataset list and select *Create New* from the pop-up menu. The *New Dataset* dialog box opens.
2. Enter the required information for the new dataset.

Name	Enter a name for the dataset.
Log Type	Select a log type from the drop-down list. • The following log types are available for FortiGate: *Application Control*, *Attack*, *DLP Archive*, *DLP*, *Email Filter*, *Event*, *Traffic*, *Virus*, *Web Filter*, and *Network Scan*. • The following log types are available for FortiMail: *Email Filter*, *Event*, *History*, and *Virus*. • The following log types are available for FortiWeb: *Attack*, *Event*, and *Traffic*.
Query	Enter the SQL query used for the dataset.
Add Variable	Select the add variable icon to add a variable, expression, and description information.
Test query with specified devices and time period	
Devices	Select *All Devices* or *Specify* to select specific devices to run the SQL query against. Use the add device icon to add multiple devices to the query.
Time Period	Use the drop-down list to select a time period. When selecting Other, enter the start date, time, end date, and time.
Test	Select Test to test the SQL query before saving the dataset configuration.

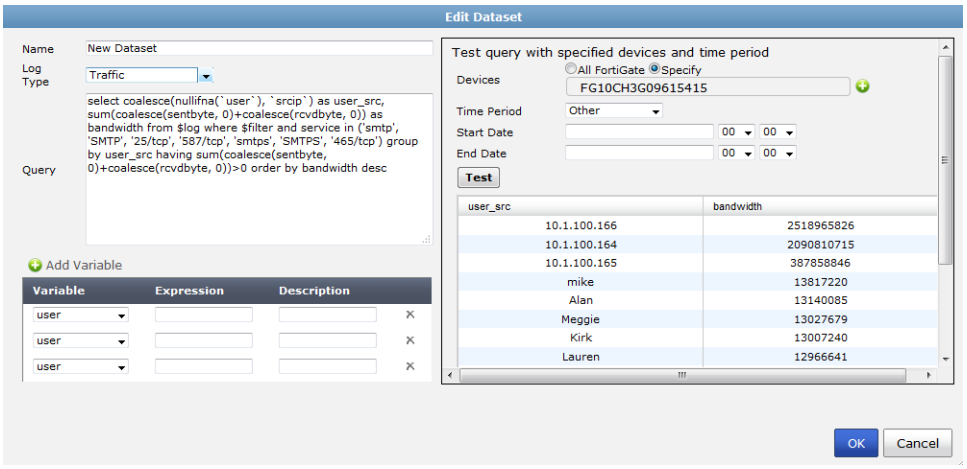
3. Test the query to ensure that the dataset functions as expected, then select *OK* to create the new dataset.

To clone a dataset:

1. In the dataset list, either select a dataset then select *Clone* from the toolbar, or right-click on the dataset then select *Clone* from the pop-up menu. The *Clone Dataset* dialog box opens.
2. Edit the information as required, then test the query to ensure that the dataset functions as expected.
3. Select *OK* to create a new, cloned dataset.

To edit a dataset:

1. In the dataset list double-click on the dataset, or select the dataset then select *Edit* from the toolbar or right-click menu. The *Edit Dataset* dialog box opens.



2. Edit the information as required, then test the query to ensure that the dataset functions as expected.
3. Select *OK* to finish editing the dataset.

Predefined 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.

To delete datasets:

1. Select the dataset or datasets that you would like to delete, then select *Delete* from the toolbar or right-click menu.
2. Select *OK* in the confirmation dialog box to delete the selected datasets or datasets.

Predefined datasets cannot be deleted, the information is read-only.

To view the SQL query for an existing dataset:

Hover the mouse cursor over one of the datasets in the dataset list. The SQL query is displayed in a persistent pop-up dialog box.

Output profile

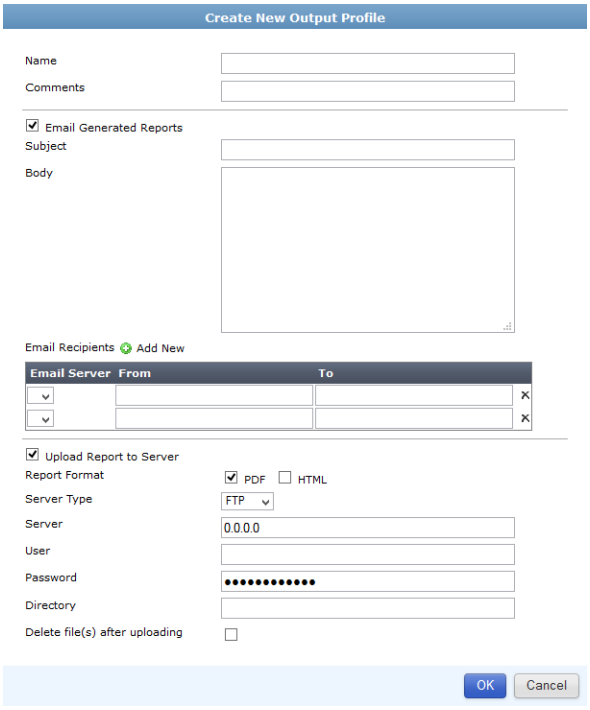
Output profiles allow you to define email addresses to which generated reports are sent, and provides an option to upload the reports to FTP, SFTP, or SCP servers. Once created, an output profile can be specified for a report.

To view and manage output profiles, go to *Reports* > *Advanced* > *Output Profile*.

You must configure a mail server before you can configure an output profile. See Mail server on page 114.

To create a new output profile:

1. In the output profile list, select *Create New* from either the toolbar or right-click menu. The *New Output Profile* dialog box opens.



2. 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 *Add New* to add another entry so that you can specify multiple recipients.
Upload Report to Server	Enable uploading the reports to a server.
Report Format	Select the report format or formats. The options include *PDF* and *HTML*.
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.

3. Select *OK* to create the new output profile.

To edit an output profile:

1. In the output profile list, 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.
2. Edit the information as required, then select *OK* to apply your changes.

To delete output profiles:

1. In the output profile list, select the output profile or profiles that you would like to delete, then select *Delete* from the toolbar or right-click menu.
2. 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 (see Advanced settings tab on page 391). New languages can be added, and the name and description of the languages can be changed. The predefined languages cannot be edited.

To view and manage report languages, go to *Reports* > *Advanced* > *Language*.

The available, pre-configured report languages include:

English (default report language)	Portuguese
French	Simplified Chinese
Japanese	Spanish
Korean	Traditional Chinese

To add a language:

1. In the report language list, select *Create New* from the toolbar or right-click menu. The *New Language* dialog box opens.
2. Enter a name and description for the language in the requisite fields.
3. 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. In the report language list, 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.
2. Edit the information as required, then select *OK* to apply your changes.

Predefined languages cannot be edited; the information is read-only.

To delete languages:

1. In the report language list, select the language or languages that you would like to delete and select *Delete* from the toolbar or right-click menu.
2. Select *OK* in the confirmation dialog box to delete the selected language or languages.

Predefined languages cannot be deleted; the information is read-only.

Appendix A - SNMP MIB Support

The FortiManager SNMP agent supports the following MIBs:

MIB or RFC	Description
FORTINET-CORE-MIB	This Fortinet-proprietary MIB enables your SNMP manager to query for system information and to receive traps that are common to multiple Fortinet devices.
FORTINET-FORTIMANAGER-FORTIANALYZER-MIB	This Fortinet-proprietary MIB enables your SNMP manager to query for FortiManager-specific information and to receive FortiManager-specific traps.
RFC-1213 (MIB II)	The FortiManager SNMP agent supports MIB II groups, except: • There is 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 FortiManager traffic activity. More accurate information can be obtained from the information reported by the FortiManager MIB.
RFC-2665 (Ethernet-like MIB)	The FortiManager SNMP agent supports Ethernet-like MIB information except the dot3Tests and dot3Errors groups.

To be able to communicate with your FortiManager unit's SNMP agent, you must first compile these MIBs into your SNMP manager. If the standard MIBs used by the SNMP agent are already compiled into your SNMP manager, you do not have to compile them again.

To view a trap or query's name, object identifier (OID), and description, open its MIB file in a plain text editor.

All traps that are sent include the message, the FortiManager unit's serial number, and the host name.

For instructions on how to configure traps and queries, see SNMP on page 107.

SNMP MIB Files

You can obtain these MIB files from the Customer Service & Support portal: https://support.fortinet.com.

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib* MIB file in the firmware image file folder. The FORTINET-CORE-MIB.mib file is located in the main FortiManager v5.00 file folder.

FORTINET-CORE-MIB

```
--
-- FORTINET-CORE-MIB.mib: Main MIB for Fortinet enterprise OID tree
```

```
--
-- MODULE-IDENTITY
--  OrgName
--     Fortinet Technologies, Inc.
--  ContactInfo
--     Technical Support
--     e-mail: support@fortinet.com
--     http://www.fortinet.com
--


FORTINET-CORE-MIB DEFINITIONS ::= BEGIN

IMPORTS
    ifIndex
        FROM IF-MIB
    InetAddress, InetAddressPrefixLength, InetAddressType
        FROM INET-ADDRESS-MIB
    MODULE-COMPLIANCE, NOTIFICATION-GROUP, OBJECT-GROUP
        FROM SNMPv2-CONF
    sysName
        FROM SNMPv2-MIB
    Integer32, MODULE-IDENTITY, NOTIFICATION-TYPE, OBJECT-TYPE,
    enterprises
        FROM SNMPv2-SMI
    DisplayString, TEXTUAL-CONVENTION
        FROM SNMPv2-TC;

fortinet MODULE-IDENTITY
    LAST-UPDATED "201205090000Z"
    ORGANIZATION
        "Fortinet Technologies, Inc."
    CONTACT-INFO
        "Technical Support
         email: support@fortinet.com
         http://www.fortinet.com
        "
    DESCRIPTION
        "Added fan failure and AMC bypass traps"
    REVISION    "201205090000Z"
    DESCRIPTION
        "Registered FortiDDoSMib OID"
    REVISION    "201204230000Z"
    DESCRIPTION
        "Registered FortiDNSMib OID"
    REVISION    "201112230000Z"
    DESCRIPTION
        "Registered FortiCacheMib OID"
    REVISION    "201104250000Z"
    DESCRIPTION
        "Supporting portuguese language"
    REVISION    "201005140000Z"
```

```
    DESCRIPTION
        "Registered FortiScanMib OID"
    REVISION    "200905200000Z"
    DESCRIPTION
        "MIB module for Fortinet network devices."
    REVISION    "200811190000Z"
    DESCRIPTION
        "Registered FortiWebMib OID"
    REVISION    "200810210000Z"
    DESCRIPTION
        "Added SMI comments"
    REVISION    "200806250000Z"
    DESCRIPTION
        "Adjusted fnAdmin tree to start at .1"
    REVISION    "200806160000Z"
    DESCRIPTION
        "Spelling corrections."
    REVISION    "200804170000Z"
    DESCRIPTION
        "Initial version of fortinet core MIB."
    ::= { enterprises 12356 }  -- assigned by IANA


--
-- Fortinet MIB Textual Conventions (TC)
--

FnBoolState ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Boolean data type representing enabled/disabled"
    SYNTAX      INTEGER {
        disabled (1),
        enabled (2)
    }

FnLanguage ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Enumerated type for user interface languages"
    SYNTAX      INTEGER {
        english (1),
        simplifiedChinese (2),
        japanese (3),
        korean (4),
        spanish (5),
        traditionalChinese (6),
        french (7),
        portuguese (8),
        undefined (255)
    }
```

```
FnIndex ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS      current
    DESCRIPTION
        "Data type for table index values"
    SYNTAX      Integer32 (0..2147483647)

FnSessionProto ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Data type for session protocols"
    SYNTAX      INTEGER {
        ip (0),
        icmp (1),
        igmp (2),
        ipip (4),
        tcp (6),
        egp (8),
        pup (12),
        udp (17),
        idp (22),
        ipv6 (41),
        rsvp (46),
        gre (47),
        esp (50),
        ah (51),
        ospf (89),
        pim (103),
        comp (108),
        raw (255)
    }

--
-- Fortinet Enterprise Structure of Management Information (SMI)
--

fnCoreMib OBJECT IDENTIFIER ::= { fortinet 100 }

--
-- Fortinet Product Family MIB Object Identifier Assignments
--
-- fnFortiGateMib     OBJECT IDENTIFIER ::= { fortinet 101 }
-- fnFortiAnalyzerMib OBJECT IDENTIFIER ::= { fortinet 102 }
-- fnFortiManagerMib  OBJECT IDENTIFIER ::= { fortinet 103 }
-- fnFortiDefenderMib OBJECT IDENTIFIER ::= { fortinet 104 }
-- fnFortiMailMib     OBJECT IDENTIFIER ::= { fortinet 105 }
-- fnFortiSwitchMib   OBJECT IDENTIFIER ::= { fortinet 106 }
-- fnFortiWebMib      OBJECT IDENTIFIER ::= { fortinet 107 }
-- fnFortiScanMib     OBJECT IDENTIFIER ::= { fortinet 108 }
-- fnFortiCacheMib    OBJECT IDENTIFIER ::= { fortinet 109 }
-- fnFortiDNSMib      OBJECT IDENTIFIER ::= { fortinet 110 }
-- fnFortiDDoSMib     OBJECT IDENTIFIER ::= { fortinet 111 }
```

```
--

--
-- fnCoreMib.fnCommon
--
fnCommon OBJECT IDENTIFIER ::= { fnCoreMib 1 }

--
-- fnCoreMib.fnCommon.fnSystem
--
fnSystem OBJECT IDENTIFIER ::= { fnCommon 1 }

fnSysSerial OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Device serial number. This is the same serial number as given
        in the ENTITY-MIB tables for the base entity."
    ::= { fnSystem 1 }

--
-- fnCoreMib.fnCommon.fnMgmt
--
fnMgmt OBJECT IDENTIFIER ::= { fnCommon 2 }

fnMgmtLanguage OBJECT-TYPE
    SYNTAX      FnLanguage
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Language used for administration interfaces"
    ::= { fnMgmt 1 }

fnAdmin OBJECT IDENTIFIER ::= { fnMgmt 100 }

fnAdminNumber OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of admin accounts in fnAdminTable"
    ::= { fnAdmin 1 }

fnAdminTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FnAdminEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of administrator accounts on the device. This table is
        intended to be extended with platform specific information."
    ::= { fnAdmin 2 }
```

```
fnAdminEntry OBJECT-TYPE
    SYNTAX      FnAdminEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable to a particular admin account"
    INDEX       { fnAdminIndex }
    ::= { fnAdminTable 1 }

FnAdminEntry ::= SEQUENCE {
    fnAdminIndex        Integer32,
    fnAdminName         DisplayString,
    fnAdminAddrType     InetAddressType,
    fnAdminAddr         InetAddress,
    fnAdminMask         InetAddressPrefixLength
}

fnAdminIndex OBJECT-TYPE
    SYNTAX      Integer32 (1..2147483647)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An index uniquely defining an administrator account within the fnAd-
minTable"
    ::= { fnAdminEntry 1 }

fnAdminName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The user-name of the specified administrator account"
    ::= { fnAdminEntry 2 }

fnAdminAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The type of address stored in fnAdminAddr, in compliance with INET-
ADDRESS-MIB"
    ::= { fnAdminEntry 3 }

fnAdminAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The address prefix identifying where the administrator account can
        be used from, typically an IPv4 address. The address type/format is
        determined by fnAdminAddrType."
```

```
    ::= { fnAdminEntry 4 }

fnAdminMask OBJECT-TYPE
    SYNTAX      InetAddressPrefixLength
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The address prefix length (or network mask) applied to the fgAdminAddr
        to determine the subnet or host the administrator can access the device
from"
    ::= { fnAdminEntry 5 }

--
-- fnCoreMib.fnCommon.fnTraps
--
fnTraps OBJECT IDENTIFIER ::= { fnCommon 3 }

fnTrapsPrefix OBJECT IDENTIFIER ::= { fnTraps 0 }

fnTrapObjects OBJECT IDENTIFIER ::= { fnTraps 1 }

fnGenTrapMsg OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Generic message associated with an event. The content will
        depend on the nature of the trap."
    ::= { fnTrapObjects 1 }

fnTrapCpuThreshold NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Indicates that the CPU usage has exceeded the configured threshold."
    ::= { fnTrapsPrefix 101 }

fnTrapMemThreshold NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Indicates memory usage has exceeded the configured threshold."
    ::= { fnTrapsPrefix 102 }

fnTrapLogDiskThreshold NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Log disk usage has exceeded the configured threshold. Only available
        on devices with log disks."
    ::= { fnTrapsPrefix 103 }
```

```
fnTrapTempHigh NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "A temperature sensor on the device has exceeded its threshold.
        Not all devices have thermal sensors. See manual for specifications."
    ::= { fnTrapsPrefix 104 }

fnTrapVoltageOutOfRange NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Power levels have fluctuated outside of normal levels. Not all devices
        have voltage monitoring instrumentation. See manual for specifications."
    ::= { fnTrapsPrefix 105 }

fnTrapPowerSupplyFailure NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Power supply failure detected. Not available on all models. Available
        on some devices which support redundant power supplies. See manual
        for specifications."
    ::= { fnTrapsPrefix 106 }

fnTrapAmcIfBypassMode NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "An AMC interface entered bypass mode. Available on models with an AMC
        expansion slot. Used with the ASM-CX4 and ASM-FX2 cards."
    ::= { fnTrapsPrefix 107 }

fnTrapFanFailure NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "A fan failure has been detected. Not all devices have fan sensors.
        See manual for specifications."
    ::= { fnTrapsPrefix 108 }

fnTrapIpChange NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, ifIndex }
    STATUS      current
    DESCRIPTION
        "Indicates that the IP address of the specified interface has been
changed."
    ::= { fnTrapsPrefix 201 }

fnTrapTest NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
```

```
    DESCRIPTION
        "Trap sent for diagnostic purposes by an administrator."
    ::= { fnTrapsPrefix 999 }

--
-- fnCoreMib.fnCommon.fnMIBConformance
--
fnMIBConformance OBJECT IDENTIFIER ::= { fnCoreMib 10 }

fnSystemComplianceGroup OBJECT-GROUP
    OBJECTS     { fnSysSerial }
    STATUS      current
    DESCRIPTION
        "Objects relating to the physical device."
    ::= { fnMIBConformance 1 }

fnMgmtComplianceGroup OBJECT-GROUP
    OBJECTS     { fnMgmtLanguage }
    STATUS      current
    DESCRIPTION
        "Objects relating the management of a device."
    ::= { fnMIBConformance 2 }

fnAdminComplianceGroup OBJECT-GROUP
    OBJECTS     { fnAdminNumber, fnAdminName, fnAdminAddrType,
                  fnAdminAddr, fnAdminMask }
    STATUS      current
    DESCRIPTION
        "Administration access control objects."
    ::= { fnMIBConformance 3 }

fnTrapsComplianceGroup NOTIFICATION-GROUP
    NOTIFICATIONS { fnTrapCpuThreshold, fnTrapMemThreshold,
                    fnTrapLogDiskThreshold, fnTrapTempHigh,
                    fnTrapVoltageOutOfRange, fnTrapPowerSupplyFailure,
                    fnTrapAmcIfBypassMode, fnTrapFanFailure,
                    fnTrapIpChange, fnTrapTest }
    STATUS      current
    DESCRIPTION
        "Event notifications"
    ::= { fnMIBConformance 4 }

fnNotifObjectsComplianceGroup OBJECT-GROUP
    OBJECTS     { fnGenTrapMsg }
    STATUS      current
    DESCRIPTION
        "Object identifiers used in notifications"
    ::= { fnMIBConformance 5 }

fnMIBCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
```

```
        "The compliance statement for the application MIB."

    MODULE      -- this module

        GROUP   fnSystemComplianceGroup
        DESCRIPTION
              "This group is mandatory for all Fortinet network appliances
              supporting this MIB."

        GROUP   fnMgmtComplianceGroup
        DESCRIPTION
              "This group is optional for devices that do not support common
              management interface options such as multiple languages."

        GROUP   fnAdminComplianceGroup
        DESCRIPTION
              "This group should be accessible on any device supporting
              administrator authentication."

        GROUP   fnTrapsComplianceGroup
        DESCRIPTION
              "Traps are optional. Not all models support all traps. Consult
              product literature to see which traps are supported."

        GROUP   fnNotifObjectsComplianceGroup
        DESCRIPTION
              "Object identifiers used in notifications. Objects are required
              if their containing trap is implemented."

    ::= { fnMIBConformance 100 }

END
```

FORTINET-FORTIMANAGER-FORTIANALYZER-MIB

```
FORTINET-FORTIMANAGER-FORTIANALYZER-MIB DEFINITIONS ::= BEGIN

IMPORTS
    fnSysSerial, fortinet, FnIndex, fnGenTrapMsg
        FROM FORTINET-CORE-MIB
    sysName
        FROM SNMPv2-MIB
    InetPortNumber
        FROM INET-ADDRESS-MIB
    MODULE-COMPLIANCE, NOTIFICATION-GROUP, OBJECT-GROUP
        FROM SNMPv2-CONF
    MODULE-IDENTITY, NOTIFICATION-TYPE, OBJECT-TYPE,
    Integer32, Gauge32, Counter32, IpAddress
        FROM SNMPv2-SMI
    DisplayString, TEXTUAL-CONVENTION
        FROM SNMPv2-TC;
```

```
fnFortiManagerMib MODULE-IDENTITY
    LAST-UPDATED "201404220000Z"
    ORGANIZATION
        "Fortinet Technologies, Inc."
    CONTACT-INFO
        "
         Technical Support
         email: support@fortinet.com
         http://www.fortinet.com"
    DESCRIPTION
         "Add model names faz3000E, fmg4000E, faz1000D, fmg1000D."
    REVISION    "201404220000Z"
    DESCRIPTION
         "Added fmSysCpuUsageExcludedNice.
          Added fmTrapCpuThresholdExcludeNice."
    REVISION    "201306100000Z"
    DESCRIPTION
         "Add support for FortiAnalyzer."
    REVISION    "201303270000Z"
    DESCRIPTION
         "Added license gb/day and device quota trap. fmTrapLicGbDayThreshold
          and fmTrapLicDevQuotaThreshold"
    REVISION    "201211260000Z"
    DESCRIPTION
         "Added commas between notifications in NOTIFICATION-GROUP.
          Added imports from SNMPv2-SMI and SNMPv2-TC.
          imported `OBJECT-GROUP' from module SNMPv2-CONF"
    REVISION    "201204200000Z"
    DESCRIPTION
         "Added RAID trap fmTrapRAIDStatusChange."
    REVISION    "201103250000Z"
    DESCRIPTION
        "Added fmSysMemUsed,fmSysMemCapacity,fmSysCpuUsage.
         Added new FortiManager models."
    REVISION    "201101190000Z"
    DESCRIPTION
        "MIB module for Fortinet FortiManager devices."
    REVISION    "200807180000Z"
    DESCRIPTION
        "Add sysName to fmTrapHASwitch."
    REVISION    "200806260000Z"
    DESCRIPTION
        "OID correction for fnFortiManagerMib."
    REVISION    "200806160000Z"
    DESCRIPTION
        "Spelling corrections."
    REVISION    "200806100000Z"
    DESCRIPTION
        "Initial version of FORTINET-FORTIMANAGER-MIB."
    ::= { fortinet 103 }
```

```
--
-- fortinet.fnFortiManagerMib.fmTraps
--

FmRAIDStatusCode ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Enumerated list of RAID status codes."
    SYNTAX      INTEGER { arrayOK(1), arrayDegraded(2), arrayFailed(3),
                   arrayRebuilding(4), arrayRebuildingStarted(5),
                   arrayRebuildingFinished(6), arrayInitializing(7),
                    arrayInitializingStarted(8), arrayInitializingFinished(9),
                    diskOk(10), diskDegraded(11), diskFailEvent(12),
        diskUnavailable(100), diskUnused(101), diskOK(102), diskRebuilding(103),
diskFailed(104), diskSpare(105),
        raidUnavailable(200), raidOK(201), raidDegraded(202), raidFailed(203),
raidBackground-Initializing(204), raidBackground-Verifying(205), raidBackground-
Rebuilding(206)}

FmSessProto ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "data type for session protocols"
    SYNTAX      INTEGER { ip(0), icmp(1), igmp(2), ipip(4), tcp(6),
                          egp(8), pup(12), udp(17), idp(22), ipv6(41),
                          rsvp(46), gre(47), esp(50), ah(51), ospf(89),
                          pim(103), comp(108), raw(255) }


fmTraps OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 0 }

fmTrapPrefix OBJECT IDENTIFIER
    ::= { fmTraps 0 }

fmTrapObject OBJECT IDENTIFIER
    ::= { fmTraps 1 }

fmRAIDStatus OBJECT-TYPE
    SYNTAX      FmRAIDStatusCode
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "New RAID state associated with a RAID status change event."
    ::= { fmTrapObject 1 }

fmRAIDDevIndex OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..32))
    MAX-ACCESS  accessible-for-notify
    STATUS      current
```

```
    DESCRIPTION
        "Name/index of a RAID device relating to the event."
    ::= { fmTrapObject 2 }

fmLogRate OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Log receiving rate in number of logs per second."
    ::= { fmTrapObject 3 }

fmLogRateThreshold OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Threshold for log rate in number of logs per second."
    ::= { fmTrapObject 4 }

fmLogDataRate OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Log receiving data rate in number of KB per second."
    ::= { fmTrapObject 5 }

fmLogDataRateThreshold OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Threshold for log data rate in number of KB per second."
    ::= { fmTrapObject 6 }

fmLicGbDay OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Log data used in number of GB per day."
    ::= { fmTrapObject 7 }

fmLicGbDayThreshold OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Licensed threshold for log data in number of GB per day."
    ::= { fmTrapObject 8 }
```

```
fmLicDevQuota OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Device quota used in number of GB."
    ::= { fmTrapObject 9 }

fmLicDevQuotaThreshold OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Licensed threshold for device quota in number of GB."
    ::= { fmTrapObject 10 }

--
-- fortinet.fnFortiManagerMib.fmModel
--

fmModel OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 1 }

fmg100 OBJECT IDENTIFIER
    ::= { fmModel 1000 }

fmgvm OBJECT IDENTIFIER
    ::= { fmModel 1001 }

fmg100C OBJECT IDENTIFIER
    ::= { fmModel 1003 }

fmg200D OBJECT IDENTIFIER
    ::= { fmModel 2004 }

fmg300D OBJECT IDENTIFIER
    ::= { fmModel 3004 }

fmg400 OBJECT IDENTIFIER
    ::= { fmModel 4000 }

fmg400A OBJECT IDENTIFIER
    ::= { fmModel 4001 }

fmg400B OBJECT IDENTIFIER
    ::= { fmModel 4002 }

fmg400C OBJECT IDENTIFIER
    ::= { fmModel 4003 }

fmg1000C OBJECT IDENTIFIER
    ::= { fmModel 10003 }
```

```
fmg1000D OBJECT IDENTIFIER
    ::= { fmModel 10004 }

fmg2000XL OBJECT IDENTIFIER
    ::= { fmModel 20000 }

fmg3000 OBJECT IDENTIFIER
    ::= { fmModel 30000 }

fmg3000B OBJECT IDENTIFIER
    ::= { fmModel 30002 }

fmg3000C OBJECT IDENTIFIER
    ::= { fmModel 30003 }

fmg3900E OBJECT IDENTIFIER
    ::= { fmModel 39005 }

fmg4000D OBJECT IDENTIFIER
    ::= { fmModel 40004 }

fmg4000E OBJECT IDENTIFIER
    ::= { fmModel 40005 }

fmg5001A OBJECT IDENTIFIER
    ::= { fmModel 50011 }

--
-- fortinet.fnFortiManagerMib.fmSystem
--

fmSystem OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 2 }

--
-- fortinet.fnFortiManagerMib.fmSystem.fmSystemInfo
--

fmSystemInfo OBJECT IDENTIFIER
    ::= { fmSystem 1 }

fmSysCpuUsage OBJECT-TYPE
    SYNTAX      Integer32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current CPU usage (percentage)"
    ::= { fmSystemInfo 1 }

fmSysMemUsed OBJECT-TYPE
    SYNTAX      Gauge32
```

```
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current memory used (KB)"
    ::= { fmSystemInfo 2 }

fmSysMemCapacity OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Total physical and swap memory installed (KB)"
    ::= { fmSystemInfo 3 }

fmSysDiskUsage OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current hard disk usage (MB)"
    ::= { fmSystemInfo 4 }

fmSysDiskCapacity OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Total hard disk capacity (MB)"
    ::= { fmSystemInfo 5 }

fmSysCpuUsageExcludedNice OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current CPU usage excluded nice processes usage (percentage)"
    ::= { fmSystemInfo 6 }

fmTrapHASwitch NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "FortiManager HA cluster has been re-arranged. A new master has been selec-
ted and asserted."
    ::= { fmTrapPrefix 401 }

fmTrapRAIDStatusChange NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName,
                      fmRAIDStatus, fmRAIDDevIndex }
    STATUS      current
    DESCRIPTION
        "Trap is sent when there is a change in the status of the RAID array, if
```

```
present."
    ::= { fmTrapPrefix 402 }

fmTrapLogAlert NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fnGenTrapMsg }
    STATUS      current
    DESCRIPTION
        "Trap is sent when a log based alert has been triggered.
         Alert description included in trap."
    ::= { fmTrapPrefix 403 }

fmTrapLogRateThreshold NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fmLogRate, fmLogRateThreshold }
    STATUS      current
    DESCRIPTION
        "Indicates that the incoming log rate has exceeded the threshold"
    ::= { fmTrapPrefix 404 }

fmTrapLogDataRateThreshold NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fmLogDataRate, fmLogDataRateThreshold }
    STATUS      current
    DESCRIPTION
        "Indicates that the incoming log data rate has exceeded the threshold"
    ::= { fmTrapPrefix 405 }

fmTrapLicGbDayThreshold NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fmLicGbDay, fmLicGbDayThreshold }
    STATUS      current
    DESCRIPTION
        "Indicates that the used log has exceeded the licensed GB/Day"
    ::= { fmTrapPrefix 407 }

fmTrapLicDevQuotaThreshold NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fmLicDevQuota, fmLicDevQuotaThreshold }
    STATUS      current
    DESCRIPTION
        "Indicates that the used device quota has exceeded the licensed device
quota"
    ::= { fmTrapPrefix 408 }

fmTrapCpuThresholdExcludeNice NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Indicates that the CPU usage excluding nice processes has exceeded the
threshold"
    ::= { fmTrapPrefix 409 }

--
-- fortinet.fnFortiManagerMib.faModel
--
```

```
faModel OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 3 }

faz100 OBJECT IDENTIFIER
    ::= { faModel 1000 }

faz100A OBJECT IDENTIFIER
    ::= { faModel 1001 }

faz100B OBJECT IDENTIFIER
    ::= { faModel 1002 }

faz100C OBJECT IDENTIFIER
    ::= { faModel 1003 }

faz200D OBJECT IDENTIFIER
    ::= { faModel 2004 }

faz300D OBJECT IDENTIFIER
    ::= { faModel 3004 }

faz400 OBJECT IDENTIFIER
    ::= { faModel 4000 }

faz400B OBJECT IDENTIFIER
    ::= { faModel 4002 }

faz400C OBJECT IDENTIFIER
    ::= { faModel 4003 }

fazvm OBJECT IDENTIFIER
    ::= { faModel 20 }

faz800 OBJECT IDENTIFIER
    ::= { faModel 8000 }

faz800B OBJECT IDENTIFIER
    ::= { faModel 8002 }

faz1000B OBJECT IDENTIFIER
    ::= { faModel 10002 }

faz1000C OBJECT IDENTIFIER
    ::= { faModel 10003 }

faz1000D OBJECT IDENTIFIER
    ::= { faModel 10004 }

faz2000 OBJECT IDENTIFIER
    ::= { faModel 20000 }

faz2000A OBJECT IDENTIFIER
```

```
    ::= { faModel 20001 }

faz2000B OBJECT IDENTIFIER
    ::= { faModel 20002 }

faz3000D OBJECT IDENTIFIER
    ::= { faModel 30004 }

faz3000E OBJECT IDENTIFIER
    ::= { faModel 30005 }

faz3500E OBJECT IDENTIFIER
    ::= { faModel 35005 }

faz3900E OBJECT IDENTIFIER
    ::= { faModel 39005 }

faz4000 OBJECT IDENTIFIER
    ::= { faModel 40000 }

faz4000A OBJECT IDENTIFIER
    ::= { faModel 40001 }

faz4000B OBJECT IDENTIFIER
    ::= { faModel 40002 }

--
-- fortinet.fnFortiManagerMib.fmInetProto
--

fmInetProto OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 4 }

fmInetProtoInfo OBJECT IDENTIFIER
    ::= { fmInetProto 1 }

fmInetProtoTables OBJECT IDENTIFIER
    ::= { fmInetProto 2 }

fmIpSessTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FmIpSessEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Information on the IP sessions active on the device"
    ::= { fmInetProtoTables 1 }

fmIpSessEntry OBJECT-TYPE
    SYNTAX      FmIpSessEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
```

```
        "Information on a specific session, including source and destination"
    INDEX       { fmIpSessIndex }
    ::= { fmIpSessTable 1 }

FmIpSessEntry ::= SEQUENCE {
    fmIpSessIndex       FnIndex,
    fmIpSessProto       FmSessProto,
    fmIpSessFromAddr    IpAddress,
    fmIpSessFromPort    InetPortNumber,
    fmIpSessToAddr      IpAddress,
    fmIpSessToPort      InetPortNumber,
    fmIpSessExp         Counter32
}

fmIpSessIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An index value that uniquely identifies
         an IP session within the fmIpSessTable"
    ::= { fmIpSessEntry 1 }

fmIpSessProto OBJECT-TYPE
    SYNTAX      FmSessProto
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The protocol the session is using (IP, TCP, UDP, etc.)"
    ::= { fmIpSessEntry 2 }

fmIpSessFromAddr OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Source IP address (IPv4 only) of the session"
    ::= { fmIpSessEntry 3 }

fmIpSessFromPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Source port number (UDP and TCP only) of the session"
    ::= { fmIpSessEntry 4 }

fmIpSessToAddr OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
```

```
        "Destination IP address (IPv4 only) of the session"
    ::= { fmIpSessEntry 5 }

fmIpSessToPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Destination Port number (UDP and TCP only) of the session"
    ::= { fmIpSessEntry 6 }

fmIpSessExp OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of seconds remaining before the session expires (if idle)"
    ::= { fmIpSessEntry 7 }

--
-- fortinet.fnFortiManagerMib.fmMibConformance
--

fmMIBConformance OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 10 }

fmTrapsComplianceGroup NOTIFICATION-GROUP
    NOTIFICATIONS { fmTrapHASwitch, fmTrapRAIDStatusChange,
                    fmTrapLogAlert, fmTrapLogRateThreshold,
                    fmTrapLogDataRateThreshold,
                    fmTrapLicGbDayThreshold,
                    fmTrapLicDevQuotaThreshold,
                    fmTrapCpuThresholdExcludeNice }
    STATUS      current
    DESCRIPTION
        "Event notifications"
    ::= { fmMIBConformance 1 }

fmSystemObjectGroup OBJECT-GROUP
    OBJECTS     { fmSysMemUsed, fmSysMemCapacity,
                  fmSysCpuUsage, fmSysDiskCapacity,
                  fmSysDiskUsage, fmSysCpuUsageExcludedNice }
    STATUS      current
    DESCRIPTION
        "Objects pertaining to the system status of the device."
    ::= { fmMIBConformance 2 }

fmNotificationObjComplianceGroup OBJECT-GROUP
    OBJECTS     { fmRAIDStatus, fmRAIDDevIndex,
                  fmLogRate, fmLogRateThreshold,
                  fmLogDataRate, fmLogDataRateThreshold,
                  fmLicGbDay, fmLicGbDayThreshold,
```

```
                  fmLicDevQuota, fmLicDevQuotaThreshold }
    STATUS      current
    DESCRIPTION
        "Object identifiers used in notifications"
    ::= { fmMIBConformance 3 }

fmSessionComplianceGroup OBJECT-GROUP
    OBJECTS {
        fmIpSessProto,
        fmIpSessFromAddr,
        fmIpSessFromPort,
        fmIpSessToAddr,
        fmIpSessToPort,
        fmIpSessExp
        }
    STATUS current
    DESCRIPTION "Session related instrumentation"
       ::= { fmMIBConformance 4 }


fmMIBCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
        "The compliance statement for the FortiManager FortiAnalyzer MIB."

    MODULE      -- this module

        GROUP   fmTrapsComplianceGroup
        DESCRIPTION
              "Traps are optional. Not all models support all traps. Consult
product literature to see which traps are supported."

        GROUP   fmSystemObjectGroup
        DESCRIPTION
              "Model and feature specific."

        GROUP   fmNotificationObjComplianceGroup
        DESCRIPTION
                 "Object identifiers used in notifications. Objects are required if
their containing trap is implemented."

        GROUP   fmSessionComplianceGroup
        DESCRIPTION
                 "IP session related implementation."

    ::= { fmMIBConformance 100 }

END -- end of module FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.
```

Appendix B - FortiManager VM

Licensing

Fortinet offers the FortiManager VM in a stackable license model. This model allows you to expand your VM solution as your environment expands. When configuring your FortiManager VM, ensure to configure hardware settings as outlined below and consider future expansion. Contact your Fortinet Authorized Reseller for more information.

Technical Specification	VM-BASE	VM-10-UG	VM-100-UG	VM-1000-UG	VM-5000-UG	VM-U-UG
Hypervisor Support	VMware ESX versions 4.0 and 4.1 VMware ESXi versions 4.0, 4.1, 5.0, 5.1, and 5.5 Microsoft Hyper-V Server 2008 R2 and 2012					
VM Form Factor	VMware ESX/ESXi: Open Virtualization Format (OVF) Microsoft Hyper-V Server: Virtual Hard Disk (VHD)					
HA Support	Yes					
Virtual CPU Support (Minimum / Maximum)	1 / Unlimited					
Network Interface Support (Minimum / Maximum)	1 / 4					
Memory Support (Minimum / Maximum)	2GB / 4GB for 32-bit and 2GB / Unlimited for 64-bit The default memory size is 2GB.					
Storage Support (Minimum / Maximum)	80GB / 16TB					
GB / Day of logs	1	2	5	10	25	50
Device Quota	100GB	200GB	1TB	4TB	8TB	16TB
Licensed Network Devices	10	+10	+100	+1000	+5000	Unlimited
Administrative Domains	10	+10	+100	+1000	+5000	Unlimited
Maximum Portal Users	10	+10	+100	+1000	+5000	Unlimited

For more information see the FortiManager product data sheet available on the Fortinet website, http://www.fortinet.com/products/fortimanager/virtualappliances.html.

Appendix C - Maximum Values

The following table provides a detailed summary of maximum values on FortiManager platforms.

FortiManager Platform	Devices/ADOMs (Maximum)	Portal Users (Maximum)
FMG-100C		
FMG-200D	30	
FMG-300D	300	
FMG-400C	300	
FMG-1000C	800	800
FMG-1000D	1,000	1,000
FMG-3000C	5,000	5,000
FMG-4000D	4,000	4,000
FMG-4000E	4,000	4,000
FMG-VM-Base	10	10
FMG-VM-10	+10	+10
FMG-VM-100	+100	+100
FMG-VM-1000	+1,000	+1,000
FMG-VM-5000	+5,000	+5,000
FMG-VM-U	Unlimited	Unlimited

Appendix D - License Information API

The FortiManager API enables you to configure managed FortiGate devices through a web services interface. See the *FortiManager XML API Reference* avaiable from the Fortinet Developer Network portal for more information.

The XML API `getDeviceLicenseList` has been added for generating and downloading license information for services on each managed device.

The data is gathered from the update manager, as opposed to individual devices in the device manager. The update manager reports what subscriptions are currently available.

The generated file contains the device serial number, and the expiry date of each service, including the support contract and various services, such as AV, IPS, and web filter.

getDeviceLicenseList

Use this request to obtain a list of device licenses.

Request Field	Description
`<servicePass>`	XML structure consists of user name and password variables.
`<userID>`	The administrator user name.
`<password>`	Administrator password options: • Type the administrator password. • Leave field blank for no password.

Example request:

```
<soapenv:Envelope xmlns:soapenv="http://..." xmlns:r20="http://.../">
   <soapenv:Header/>
   <soapenv:Body>
      <r20:getDeviceLicenseList>
         <!--Optional:-->
         <servicePass>
            <!--Optional:-->
            <userID>admin</userID>
            <!--Optional:-->
            <password></password>
         </servicePass>
      </r20:getDeviceLicenseList>
   </soapenv:Body>
</soapenv:Envelope>
```

The response includes the device serial number, support type, support level, and expiry date.

Response Field	Description
<serial_number>	The device serial number.
<support_type>	Support contract types include: • AVDB: Antivirus Signature Definition Update Support • AVEN: Antivirus Engine Update Support • COMP: Comprehensive Support • ENHN: Enhancement Support • FMWR: Firmware Update Support • FRVS: FortiScanner Database Update Support • FURL: Web Filtering Support • SPAM: AntiSpam Support • HDWR: Hardware Support • NIDS: Intrusion Detection Support • SPRT: Technical Support via Telephone • VCME: FortiGate Network scanner plugin
<support_level>	Support levels include: • 99: Trial contract • 10: 8x5 support contract • 20: 24x7 support contract
<expiry_date>	Support contract expiry date.

Example response

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getDeviceLicenseListResponse>
      <return>
         <device>
            <serial_number>FE100C3909000002</serial_number>
            <contract>
               <support_type>AVDB</support_type>
               <support_level>10</support_level>
               <expiry_date>20120824</expiry_date>
            </contract>
            <contract>
               <support_type>AVEN</support_type>
               <support_level>10</support_level>
               <expiry_date>20120824</expiry_date>
            </contract>
            <contract>
               <support_type>NIDS</support_type>
               <support_level>10</support_level>
               <expiry_date>20120824</expiry_date>
            </contract>
            <contract>
               <support_type>SPAM</support_type>
               <support_level>10</support_level>
```

```
            <expiry_date>20120824</expiry_date>
         </contract>
         <contract>
            <support_type>SPRT</support_type>
            <support_level>20</support_level>
            <expiry_date>20120824</expiry_date>
         </contract>
         <contract>
            <support_type>FRVS</support_type>
            <support_level>10</support_level>
            <expiry_date>20120824</expiry_date>
         </contract>
      </device>
   </return>
</ns3:getDeviceLicenseListResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Appendix E - Charts, Datasets, & Macros

FortiGate

Predefined charts

The following table lists the predefined charts for FortiGate.

Name	Description	Category
Active Traffic Users	List of active traffic users	Traffic
Admin Login Summary by Date	Administrator login summary by date	Event
Adware Timeline	Adware timeline	Virus
Application Bandwidth Usage	Application bandwidth usage details	Traffic
Application Risk Distribution	Application risk distribution	Traffic
Applications Running over HTTP	Applications running over HTTP protocol	Traffic
Attack Summary	Intrusion events summary	Attack
Attacks Over HTTP/HTTPs	Intrusions over HTTP or HTTPs	Attack
Bandwidth Summary	Traffic bandwidth usage summary	Traffic
Botnet Timeline	Botnet timeline	Traffic
Botnet Victims	Botnet victims	Traffic
Browsing Time Summary	Browsing time summary	Traffic
Browsing Time Summary Enhanced	Enhanced browsing time summary	Traffic
CPU Session Usage	CPU session usage	Event
CPU Usage	CPU usage	Event
Detailed Web Browsing Log	Detailed browsing log of web	Traffic
Detected Botnets	Detected botnets	Traffic
Detected OS Count	Detected operating system count	Traffic

Name	Description	Category
Distribution of SIP Calls by Duration	Distribution of SIP calls by duration	DLP Archive
Hourly Category and Website Hits	Hourly category and website hits	Traffic
Intrusions Timeline	Intrusions timeline by severity	Attack
Managed AP Summary Pie Chart	Managed wireless access point summary by status pie chart	Event
Memory Usage	Memory usage	Event
Number of Applications by Risk Behaviour	Number of applications by risk behaviour	Traffic
Number of Distinct WiFi Clients	Number of distinct WiFi clients	Traffic
Number of SCCP Call Registrations by Hour-of-Day	Number of SCCP call registrations by hour of day	DLP Archive
Number of SCCP Calls by Status	Number of SCCP calls by status	DLP Archive
Number of SIP Call Registrations by Hour-of-Day	Number of SIP call registrations by hour of day	DLP Archive
Number of SIP Calls by Status	Number of SIP calls by status	DLP Archive
Off-Wire Rogue APs	Rogue off-wire wireless access points	Event
SCCP Call Duration by Hour-of-Day	SCCP call duration by hour of day	DLP Archive
Session History Graph	Session history graph	Traffic
Session Summary	Session summary	Traffic
Session Usage	Session usage	Event
Spyware Timeline	Spyware timeline	Virus
System Events Summary by Date	System events summary by date	Event
Threat Incident Summary	Number of incidents for all users and devices	Traffic
Threat Score Summary	Threat score summary for all users and devices	Traffic
Top 10 Destination Countries by Browsing Time Enhanced	Top 10 destination countries by enhanced browsing time	Traffic

Name	Description	Category
Top 100 Critical Severity System Events	Top 100 critical severity system events	Event
Top 100 High Severity System Events	Top 100 high severity system events	Event
Top 100 Medium Severity System Events	Top 100 medium severity system events	Event
Top 100 Off-Wire Accepted APs	Top 100 off-wire accepted wireless access points	Event
Top 100 Off-Wire Suppressed APs	Top 100 suppressed off-wire wireless access points	Event
Top 100 Off-Wire Unclassified APs	Top 100 unclassified off-wire wireless access points	Event
Top 100 On-Wire Accepted APs	Top 100 on-wire accepted wireless access points	Event
Top 100 On-Wire Rogue APs	Top 100 rogue on-wire wireless access points	Event
Top 100 On-Wire Suppressed APs	Top 100 suppressed on-wire wireless access points	Event
Top 100 On-Wire Unclassified APs	Top 100 unclassified on-wire wireless access points	Event
Top 100 WiFi Client Details	Top 100 details of client event of wireless access point	Event
Top 15 Destination Countries by Browsing Time	Top 15 destination countries by browsing time	Traffic
Top 15 Websites by Browsing Time	Top 15 websites by browsing time	Traffic
Top 20 Admin Login Summary	Top 20 login summary of administrator	Event
Top 20 Allowed Web Categories	Top 20 allowed web filtering categories	Web Filter
Top 20 Application Categories by Bandwidth	Top 20 application categories by bandwidth usage	Web Filter
Top 20 Bandwidth Users	Top 20 web users by bandwidth users	Web Filter
Top 20 Blocked Intrusions	Top 20 blocked intrusions	Attack
Top 20 Blocked Web Categories	Top 20 blocked web filtering categories	Web Filter

Name	Description	Category
Top 20 Category and Applications by Bandwidth	Top 20 category and applications by bandwidth usage	Traffic
Top 20 Category and Applications by Sessions	Top 20 category and applications by session count	Traffic
Top 20 Category and Websites by Bandwidth	Top 20 category and websites by bandwidth usage	Traffic
Top 20 Category and Websites by Sessions	Top 20 category and websites by session count	Traffic
Top 20 Critical Severity Intrusions	Top 20 critical severity intrusions	Attack
Top 20 Failed Admin Logins	Top 20 failed logins of administrator	Event
Top 20 High Risk Applications	Top 20 high risk applications	Traffic
Top 20 High Severity Intrusions	Top 20 high severity intrusions	Attack
Top 20 Intrusion Sources	Top 20 intrusion sources	Attack
Top 20 Intrusion Victims	Top 20 intrusion victims	Attack
Top 20 Intrusions by Types	Top 20 intrusions by types	Attack
Top 20 Low Severity Intrusions	Top 20 low severity intrusions	Attack
Top 20 Medium Severity Intrusions	Top 20 medium severity intrusions	Attack
Top 20 Monitored Intrusions	Top 20 monitored intrusions	Attack
Top 20 Users by Bandwidth	Top 20 users by bandwidth usage	Traffic
Top 20 Users or Sources by Sessions	Top 20 users or sources by session count	Traffic
Top 20 Virus Victims	Top 20 virus victims	Traffic
Top 20 Viruses	Top 20 viruses detected	Traffic
Top 20 Web Categories by Bandwidth and Sessions	Top 20 web filtering categories by bandwidth usage and session count	Traffic
Top 20 Web Domains by Visits	Top 20 visited web domains by number of visits	Traffic
Top 20 Web Users by Requests	Top 20 web users by number of requests	Traffic

Name	Description	Category
Top 30 Application Categories by Bandwidth	Top 30 application categories by bandwidth usage	Traffic
Top 30 Applications by Bandwidth and Sessions	Top 30 applications by bandwidth usage and session count	Traffic
Top 30 Destinations by Bandwidth and Sessions	Top 30 destinations by bandwidth usage and session count	Traffic
Top 30 Key Applications	Top 30 key applications crossing the network	Traffic
Top 30 Users by Bandwidth and Sessions	Top 30 users by bandwidth usage and session count	Traffic
Top 5 Attacks by Severity	Top 5 attacks by severity	Attack
Top 5 IPS Events by Severity	Top 5 intrusion protection events by severity	Attack
Top 5 System Events by Severity	Top 5 system events summary by severity	Event
Top 5 Users by Bandwidth	Top 5 users by bandwidth usage	Traffic
Top 50 Allowed Websites	Top 50 allowed websites by number of requests	Web Filter
Top 50 Allowed Websites by Requests	Top 50 allowed websites by number of requests	Traffic
Top 50 Websites and Category by Bandwidth	Top 50 websites and web filtering categories by bandwidth usage	Web Filter
Top 50 Websites by Browsing Time	Top 50 websites by browsing time	Traffic
Top 50 Websites by Browsing Time Enhanced	Top 50 websites by enhanced browsing time	Traffic
Top 500 Allowed Applications by Bandwidth	Top 500 allowed applications by bandwidth usage	Traffic
Top 500 Blocked Applications by Sessions	Top 500 blocked applications by session count	Traffic
Top 500 Websites by Bandwidth	Top 500 website sessions by bandwidth usage	Traffic
Top Adware	Top 10 adware	Virus

Name	Description	Category
Top Adware Sources	Top 10 adware sources	Traffic
Top Adware Victims	Top 10 adware victims	Virus
Top Allowed Websites by Bandwidth	Top 10 allowed websites by bandwidth usage	Traffic
Top Application Categories Bandwidth Pie Chart	Top 10 application categories by bandwidth usage pie chart	Traffic
Top Application Categories by Bandwidth	Top 10 application categories by bandwidth usage	Traffic
Top Application Vulnerabilities	Top 10 application vulnerabilities discovered	Network Scan
Top Applications by Bandwidth	Top 10 applications by bandwidth usage	Traffic
Top Applications by Sessions	Top 10 applications by session count	Traffic
Top Applications by WiFi Traffic	Top 10 applications by WiFi bandwidth usage	Traffic
Top APs by Bandwidth	Top 10 wireless access points by WiFi bandwidth usage	Traffic
Top APs by WiFi Clients	Top 10 wireless access points by number of clients via WiFi	Traffic
Top Attack Sources	Top 10 attack sources	Attack
Top Attack Victims	Top 10 attack victims	Attack
Top Attacks	Top 10 intrusions	Attack
Top Authenticated VPN Logins	Top 10 authenticated VPN logins	Event
Top Blocked Attacks	Top 10 blocked intrusions	Attack
Top Blocked SCCP Callers	Top 10 blocked SCCP callers	Application Control
Top Blocked SIP Callers	Top 10 blocked SIP callers	Application Control
Top Blocked Web Users	Top 10 blocked web users	Traffic
Top Blocked Websites	Top 10 blocked websites by number of requests	Traffic

Name	Description	Category
Top Blocked Websites and Categories	Top 10 blocked web filtering websites and categories by number of requests	Web Filter
Top Botnet Infected Hosts	Top 10 botnet infected hosts	Traffic
Top Botnet Sources	Top 10 botnet sources	Traffic
Top Botnets by Sources	Top 10 botnets by sources	Traffic
Top Critical Severity IPS Events	Top 10 critical severity intrusion protection events	Attack
Top Destination Countries by Browsing Time	Top 10 destination countries by browsing time	Traffic
Top Destination Countries by Browsing Time Enhanced	Top destination countries by browsing time	Traffic
Top Destinations by Bandwidth	Top 10 destination addresses by bandwidth usage	Traffic
Top Destinations by Sessions	Top 10 destination addresses by session count	Traffic
Top Device Types by WiFi Clients	Top 10 device types by number of clients via WiFi	Traffic
Top Device Types by WiFi Traffic	Top 10 device types by WiFi bandwidth usage	Traffic
Top Devices by Increased Threat Scores	Top 10 devices by increased threat scores for last two periods	Traffic
Top Devices by Threat Score	Top 10 devices by threat score in risk	Traffic
Top Devices by Threat Scores	Top 10 devices by threat scores	Traffic
Top DHCP Summary by Interfaces	Top 10 DHCP summary by interfaces	Event
Top Dial-up IPsec Tunnels by Bandwidth	Top 10 dial-up IPsec VPN tunnels by bandwidth usage	Event
Top Dial-up IPsec Users by Bandwidth	Top 10 users of dial-up IPsec VPN by bandwidth usage	Event
Top Dial-up IPsec Users by Bandwidth and Availability	Top 10 users of dial-up IPsec VPN tunnel by bandwidth usage and availability	Event

Name	Description	Category
Top Dial-up IPsec Users by Duration	Top 10 users of dial-up IPsec VPN by duration	Event
Top Dial-up VPN Users by Duration	Top 10 users of dial-up SSL and IPsec VPN by duration	Event
Top DLP Events	Top 10 data leak prevention events	Traffic
Top Email Recipients	Top 10 recipients by number of emails	Traffic
Top Email Senders	Top 10 senders by number of emails	Traffic
Top Failed VPN Logins	Top 10 failed VPN login attempts	Event
Top High Severity IPS Events	Top 10 high severity intrusion protection events	Attack
Top Informational Severity IPS Events	Top 10 informational severity intrusion protection events	Attack
Top IPsec Dial-up User by Bandwidth	Top 10 users of IPsec VPN dial-up tunnel by bandwidth usage	Event
Top Low Severity IPS Events	Top 10 low severity intrusion protection events	Attack
Top Malware	Top malware detected by malware type	Traffic
Top Malware Sources	Top 10 malware sources by host name or IP address	Traffic
Top Managed AP Summary	Top 10 managed wireless access point summary by status	Event
Top Medium Severity IPS Events	Top 10 medium severity intrusion protection events	Attack
Top Off-Wire AP Details	Top 10 details of off-wire wireless access point	Event
Top Off-Wire AP Summary	Top 10 default off-wire wireless access point detection summary by status	Event
Top Off-Wire AP Summary Pie Chart	Top 10 off-wire wireless access point detection summary by status pie chart	Event
Top On-Wire AP Details	Top 10 details of on-wire wireless access point	Event

Name	Description	Category
Top On-Wire AP Summary	Top 10 default on-wire wireless access point detection summary by status	Event
Top On-Wire AP Summary Pie Chart	Top 10 default on-wire wireless access point detection summary by status pie chart	Event
Top OS by WiFi Clients	Top 10 operating systems by number of clients via WiFi	Traffic
Top OS by WiFi Traffic	Top 10 operating systems by WiFi bandwidth usage	Traffic
Top Recipients by Aggregated Email Size	Top 10 recipients by aggregated email size	Traffic
Top Search Phrases	Top 10 search filtering phrases	Web Filter
Top Senders by Aggregated Email Size	Top 10 senders by aggregated email size	Traffic
Top Site-to-Site IPsec Tunnels by Bandwidth	Top 10 site-to-site IPsec VPN tunnels by bandwidth usage	Event
Top Site-to-Site IPsec Tunnels by Bandwidth and Availability	Top 10 Site-to-Site IPsec tunnels by bandwidth usage and availability	Event
Top Spyware	Top 10 spyware	Virus
Top Spyware Sources	Top 10 spyware sources	Traffic
Top Spyware Victims	Top 10 spyware victims	Virus
Top SSIDs by Bandwidth	Top 10 SSIDs by WiFi bandwidth usage	Traffic
Top SSIDs by WiFi Clients	Top 10 SSIDs by number of clients via WiFi	Traffic
Top SSL Tunnel Users by Bandwidth	Top 10 users of SSL VPN tunnel by bandwidth usage	Event
Top SSL Tunnel Users by Bandwidth and Availability	Top 10 users of SSL VPN tunnel by bandwidth usage and availability	Event
Top SSL Users by Duration	Top 10 users of SSL VPN web portal and tunnel by duration	Event
Top SSL VPN Sources by Bandwidth	Top 10 users of SSL VPN tunnel by bandwidth usage	Event
Top SSL Web Portal Users by Bandwidth	Top 10 users of SSL VPN web portal by bandwidth usage	Event

Name	Description	Category
Top SSL Web Portal Users by Bandwidth and Availability	Top 10 users of SSL web portal by bandwidth usage and availability	Event
Top Unclassified AP Summary	Top 10 unclassified wireless access point summary by status	Event
Top Users Browsing Time Bar Chart	Top 10 users by estimated web browsing time bar chart	Traffic
Top Users Browsing Time Enhanced	Top 10 users by enhanced estimated web browsing time	Traffic
Top Users by Bandwidth	Top 10 users by bandwidth usage	Traffic
Top Users by Browsing Time	Top 10 users by estimated web browsing time	Traffic
Top Users by Browsing Time Enhanced	Top users by enhanced estimated web browsing time	Traffic
Top Users by Increased Threat Scores	Top 10 users by increased threat scores for last 2 periods	Traffic
Top Users by Sessions	Top 10 users by session count	Traffic
Top Users by Threat Scores	Top 10 users by threat scores	Traffic
Top Users Threat Score Bar Chart	Top 10 users by threat score bar chart	Traffic
Top Video Streaming Applications and Websites by Bandwidth	Top 10 video streaming applications and websites by bandwidth usage	Traffic
Top Video Streaming Websites by Bandwidth	Top 10 video streaming websites of web filter by bandwidth usage	Web Filter
Top Virus Victims	Top virus victims	Traffic
Top Viruses	Top 10 viruses detected	Traffic
Top Web Categories by Bandwidth and Sessions	Top 10 web filtering categories by bandwidth usage and session count	Traffic
Top Web Categories by Browsing Time	Top 10 web filtering categories by browsing time	Traffic
Top Web Categories by Browsing Time Enhanced	Top 10 web filtering categories by enhanced browsing time	Traffic

Name	Description	Category
Top Web Users by Allowed Requests	Top 10 web users by number of allowed requests	Web Filter
Top Web Users by Bandwidth	Top 10 web users by bandwidth usage	Traffic
Top Web Users by Blocked Requests	Top 10 web users by number of blocked requests	Web Filter
Top Websites by Browsing Time Enhanced	Top websites by enhanced browsing time	Traffic
Top WiFi Clients Bandwidth Bar Chart	Top 10 WiFi clients by bandwidth usage bar chart	Traffic
Top WiFi Clients by Bandwidth	Top 10 clients by WiFi bandwidth usage	Traffic
Traffic History	Traffic history by number of active users	Traffic
Traffic Statistics	Top 10 traffic statistics summary	Traffic
Unclassified AP Summary Pie Chart	Unclassified wireless access point summary by status pie chart	Event
User Top 500 Websites by Bandwidth	Top 500 user visted websites by bandwidth usage	Traffic
User Top 500 Websites by Sessions	Top 500 user visted websites by session count	Traffic
Virus Timeline	Virus timeline	Virus
Viruses Discovered	Viruses discovered	Traffic
VPN Logins	List of VPN user logins	Event
VPN Traffic Usage Trend	Bandwidth usage trend for VPN traffic	Event
Web Activity Summary	Web activity summary by number of requests	Web Filter
WiFi Traffic Bandwidth	Overall WiFi traffic bandwidth usage	Traffic

Predefined datasets

The following table lists the predefined datasets for FortiGate.

Name	Log Type
App-Risk-App-Usage-By-Category	Traffic
App-Risk-Application-Activity-APP	Traffic
App-Risk-Applications-Running-Over-HTTP	Traffic
App-Risk-Breakdown-Of-Risk-Applications	Traffic
App-Risk-DLP-UTM-Event	Traffic
App-Risk-High-Risk-Application	Traffic
App-Risk-Number-Of-Applications-By-Risk-Behavior	Traffic
App-Risk-Reputation-Top-Devices-By-Scores	Traffic
App-Risk-Reputation-Top-Users-By-Scores	Traffic
App-Risk-Top-Critical-Threat-Vectors	Attack
App-Risk-Top-High-Threat-Vectors	Attack
App-Risk-Top-Info-Threat-Vectors	Attack
App-Risk-Top-Low-Threat-Vectors	Attack
App-Risk-Top-Medium-Threat-Vectors	Attack
App-Risk-Top-Threat-Vectors	Attack
App-Risk-Top-User-Source-By-Sessions	Traffic
App-Risk-Virus-Discovered	Traffic
App-Risk-Vulnerability-Discovered	Network Scan
App-Risk-Web-Browsing-Activity-Hostname-Category	Traffic
App-Risk-Web-Browsing-Summary-Category	Traffic
App-Sessions-By-Category	Traffic
app-Top-Allowed-Applications-by-Bandwidth	Traffic
app-Top-Blocked-Applications-by-Session	Traffic
app-Top-Category-and-Applications-by-Bandwidth	Traffic

Name	Log Type
app-Top-Category-and-Applications-by-Session	Traffic
appctrl-Top-Blocked-SCCP-Callers	Application Control
appctrl-Top-Blocked-SIP-Callers	Application Control
Application-Session-History	Traffic
bandwidth-app-Top-Dest-By-Bandwidth-Sessions	Traffic
bandwidth-app-Top-Users-By-Bandwidth	Traffic
bandwidth-app-Traffic-By-Active-User-Number	Traffic
bandwidth-app-Traffic-Statistics	Traffic
Botnet-Activity-By-Sources	Traffic
Botnet-Infected-Hosts	Traffic
Botnet-Sources	Traffic
Botnet-Timeline	Traffic
Botnet-Victims	Traffic
content-Count-Total-SCCP-Call-Registrations-by-Hour-of-Day	DLP Archive
content-Count-Total-SCCP-Calls-Duration-by-Hour-of-Day	DLP Archive
content-Count-Total-SCCP-Calls-per-Status	DLP Archive
content-Count-Total-SIP-Call-Registrations-by-Hour-of-Day	DLP Archive
content-Count-Total-SIP-Calls-per-Status	DLP Archive
content-Dist-Total-SIP-Calls-by-Duration	DLP Archive
default-AP-Detection-Summary-by-Status-OffWire	Event
default-AP-Detection-Summary-by-Status-OnWire	Event
default-Email-Top-Receivers-By-Bandwidth	Traffic
default-Email-Top-Receivers-By-Count	Traffic
default-Email-Top-Senders-By-Bandwidth	Traffic

Name	Log Type
default-Managed-AP-Summary	Event
default-selected-AP-Details-OffWire	Event
default-selected-AP-Details-OnWire	Event
default-Top-Dial-Up-User-Of-Vpn-Tunnel-By-Bandwidth	Traffic
default-Top-Email-Senders-By-Count	Traffic
default-Top-IPSEC-Vpn-Dial-Up-User-By-Bandwidth	Event
default-Top-Sources-Of-SSL-VPN-Tunnels-By-Bandwidth	Event
default-Unclassified-AP-Summary	Event
Detailed-Application-Usage	Traffic
Detected-Botnet	Traffic
drilldown-Top-App-By-Bandwidth	Traffic
drilldown-Top-App-By-Sessions	Traffic
drilldown-Top-Attack-Dest	Attack
drilldown-Top-Attack-List	Attack
drilldown-Top-Attack-Source	Attack
drilldown-Top-Destination-By-Bandwidth	Traffic
drilldown-Top-Destination-By-Sessions	Traffic
drilldown-Top-Email-Receive-Sender-By-Count	Traffic
drilldown-Top-Email-Receive-Sender-By-Volume	Traffic
drilldown-Top-Email-Receiver-By-Count	Traffic
drilldown-Top-Email-Receiver-By-Volume	Traffic
drilldown-Top-Email-Send-Recipient-By-Count	Traffic
drilldown-Top-Email-Send-Recipient-By-Volume	Traffic
drilldown-Top-Email-Sender-By-Count	Traffic

Name	Log Type
drilldown-Top-Email-Sender-By-Volume	Traffic
drilldown-Top-User-By-Bandwidth	Traffic
drilldown-Top-User-By-Sessions	Traffic
drilldown-Top-Web-User-By-Visit	Traffic
drilldown-Top-Website-By-Request	Traffic
drilldown-Virus-Detail	Traffic
Estimated-Browsing-Time	Traffic
event-Admin-Failed-Login-Summary	Event
event-Admin-Login-Summary	Event
event-Admin-Login-Summary-By-Date	Event
event-System-Critical-Severity-Events	Event
event-System-High-Severity-Events	Event
event-System-Medium-Severity-Events	Event
event-System-Summary-By-Date	Event
event-System-Summary-By-Severity	Event
event-Top-DHCP-Summary	Event
event-Usage-CPU	Event
event-Usage-CPU-Sessions	Event
event-Usage-Mem	Event
event-Usage-Sessions	Event
event-Wireless-Accepted-Offwire	Event
event-Wireless-Accepted-Onwire	Event
event-Wireless-Client-Details	Event
event-Wireless-Rogue-Offwire	Event

Name	Log Type
event-Wireless-Rogue-Onwire	Event
event-Wireless-Suppressed-Offwire	Event
event-Wireless-Suppressed-Onwire	Event
event-Wireless-Unclassified-Offwire	Event
event-Wireless-Unclassified-Onwire	Event
High-Risk-Application-By-Bandwidth	Traffic
High-Risk-Application-By-Sessions	Traffic
number-of-session-timeline	Traffic
os-Detect-OS-Count	Traffic
reputation-Number-Of-Incidents-For-All-Users-Devices	Traffic
reputation-Score-Summary-For-All-Users-Devices	Traffic
reputation-Top-Devices-By-Scores	Traffic
reputation-Top-Devices-With-Increased-Scores	Traffic
reputation-Top-Users-By-Scores	Traffic
reputation-Top-Users-With-Increased-Scores	Traffic
threat-Adware-Timeline	Virus
threat-Attacks-By-Severity	Attack
threat-Attacks-Over-HTTP-HTTPs	Attack
threat-Critical-Severity-Intrusions	Attack
threat-High-Severity-Intrusions	Attack
threat-Intrusion-Timeline	Attack
threat-Intrusions-Timeline-By-Severity	Attack
threat-Low-Severity-Intrusions	Attack
threat-Medium-Severity-Intrusions	Attack

Name	Log Type
threat-Spyware-Timeline	Virus
threat-Top-Adware-by-Name	Virus
threat-Top-Adware-Source	Traffic
threat-Top-Adware-Victims	Virus
threat-Top-Attacks-Blocked	Attack
threat-Top-Attacks-Detected	Attack
threat-Top-Blocked-Intrusions	Attack
threat-Top-Intrusion-Sources	Attack
threat-Top-Intrusion-Victims	Attack
threat-Top-Intrusions-By-Types	Attack
threat-Top-Monitored-Intrusions	Attack
threat-Top-Spyware-by-Name	Virus
threat-Top-Spyware-Source	Traffic
threat-Top-Spyware-Victims	Virus
threat-Top-Virus-Source	Traffic
threat-Virus-Timeline	Virus
Top-App-By-Bandwidth	Traffic
Top-App-By-Sessions	Traffic
Top-Destinations-By-Bandwidth	Traffic
Top-Destinations-By-Sessions	Traffic
Top-P2P-App-By-Bandwidth	Traffic
Top-P2P-App-By-Sessions	Traffic
Top-User-By-Sessions	Traffic
Top-User-Source-By-Sessions	Traffic

Name	Log Type
Top-Users-By-Bandwidth	Traffic
Top-Web-Category-by-Bandwidth	Web Filter
Top-Web-Category-by-Sessions	Web Filter
Top-Web-Sites-by-Bandwidth	Web Filter
Top-Web-Sites-by-Sessions	Web Filter
Total-Attack-Source	Attack
Total-Number-of-Botnet-Events	Traffic
Total-Number-of-Viruses	Traffic
traffic-bandwidth-timeline	Traffic
traffic-Browsing-Time-Summary	Traffic
Traffic-History-By-Active-User	Traffic
traffic-Top-Category-By-Browsing-Time	Traffic
traffic-Top-Destination-Countries-By-Browsing-Time	Traffic
traffic-Top-Domains-By-Browsing-Time	Traffic
traffic-Top-Sites-By-Browsing-Time	Traffic
traffic-Top-Users-By-Bandwidth	Traffic
traffic-Top-WiFi-Client-By-Bandwidth	Traffic
user-drilldown-Count-Spam-Activity-by-Hour-of-Day	Email Filter
user-drilldown-Top-Allowed-Web-Categories	Web Filter
user-drilldown-Top-Allowed-Web-Sites-By-Requests	Web Filter
user-drilldown-Top-Attacks-By-Name	Attack
user-drilldown-Top-Attacks-High-Severity	Attack
user-drilldown-Top-Blocked-Web-Categories	Web Filter
user-drilldown-Top-Blocked-Web-Sites-By-Requests	Web Filter

Name	Log Type
user-drilldown-Top-Spam-Sources	Email Filter
user-drilldown-Top-Virus	Virus
user-drilldown-Top-Virus-Receivers-Over-Email	Virus
utm-drilldown-Email-Receivers-Summary	Traffic
utm-drilldown-Email-Senders-Summary	Traffic
utm-drilldown-Top-Allowed-Web-Sites-By-Request	Traffic
utm-drilldown-Top-App-By-Bandwidth	Traffic
utm-drilldown-Top-App-By-Sessions	Traffic
utm-drilldown-Top-Attacks-By-Name	Attack
utm-drilldown-Top-Blocked-Web-Sites-By-Request	Traffic
utm-drilldown-Top-Email-Recipients	Traffic
utm-drilldown-Top-Email-Senders	Traffic
utm-drilldown-Top-User-Destination	Traffic
utm-drilldown-Top-Users-By-Bandwidth	Traffic
utm-drilldown-Top-Virus	Traffic
utm-drilldown-Top-Vulnerability-By-Name	Network Scan
utm-drilldown-Traffic-Summary	Traffic
utm-Top-Allowed-Web-Sites-By-Request	Traffic
utm-Top-Allowed-Websites-By-Bandwidth	Traffic
utm-Top-Attack-Dest	Attack
utm-Top-Attack-Source	Attack
utm-Top-Blocked-Web-Sites-By-Request	Traffic
utm-Top-Blocked-Web-Users	Traffic
utm-Top-Video-Streaming-Websites-By-Bandwidth	Traffic

Name	Log Type
utm-Top-Virus	Traffic
utm-Top-Virus-User	Traffic
utm-Top-Web-Users-By-Bandwidth	Traffic
utm-Top-Web-Users-By-Request	Traffic
vpn-Authenticated-Logins	Event
vpn-Failed-Logins	Event
vpn-Top-Dial-Up-IPSEC-Tunnels-By-Bandwidth	Event
vpn-Top-Dial-Up-IPSEC-Users-By-Bandwidth	Event
vpn-Top-Dial-Up-IPSEC-Users-By-Duration	Event
vpn-Top-Dial-Up-VPN-Users-By-Duration	Event
vpn-Top-Dialup-IPSEC-Users-By-Bandwidth-and-Avail	Event
vpn-Top-S2S-IPSEC-Tunnels-By-Bandwidth-and-Avail	Event
vpn-Top-SSL-Tunnel-Users-By-Bandwidth-and-Avail	Event
vpn-Top-SSL-VPN-Tunnel-Users-By-Bandwidth	Event
vpn-Top-SSL-VPN-Users-By-Bandwidth	Event
vpn-Top-SSL-VPN-Users-By-Duration	Event
vpn-Top-SSL-VPN-Web-Mode-Users-By-Bandwidth	Event
vpn-Top-SSL-Web-Users-By-Bandwidth-and-Avail	Event
vpn-Top-Static-IPSEC-Tunnels-By-Bandwidth	Traffic
vpn-Traffic-Usage-Trend-VPN	Event
vpn-User-Login-history	Event
web-Detailed-Website-Browsing-Log	Traffic
web-Hourly-Category-and-Website-Hits-Action	Traffic
web-Top-Category-and-Websites-by-Bandwidth	Traffic

Name	Log Type
web-Top-Category-and-Websites-by-Session	Traffic
web-Top-User-Visted-Websites-by-Bandwidth	Traffic
web-Top-User-Visted-Websites-by-Session	Traffic
web-Top-Website-Sessions-by-Bandwidth	Traffic
webfilter-Categories-By-Bandwidth	Web Filter
webfilter-Top-Allowed-Web-Categories	Web Filter
webfilter-Top-Allowed-Web-Sites-by-Bandwidth	Web Filter
webfilter-Top-Allowed-Web-Sites-By-Requests	Web Filter
webfilter-Top-Blocked-Web-Categories	Web Filter
webfilter-Top-Blocked-Web-Sites-By-Requests	Web Filter
webfilter-Top-Search-Phrases	Web Filter
webfilter-Top-Video-Streaming-Websites-By-Bandwidth	Web Filter
webfilter-Top-Web-Users-By-Allowed-Requests	Web Filter
webfilter-Top-Web-Users-By-Bandwidth	Web Filter
webfilter-Top-Web-Users-By-Blocked-Requests	Web Filter
webfilter-Web-Activity-Summary-By-Requests	Web Filter
wifi-Num-Distinct-Client	Traffic
wifi-Overall-Traffic	Traffic
wifi-Top-AP-By-Bandwidth	Traffic
wifi-Top-AP-By-Client	Traffic
wifi-Top-App-By-Bandwidth	Traffic
wifi-Top-Client-By-Bandwidth	Traffic
wifi-Top-Device-By-Bandwidth	Traffic
wifi-Top-Device-By-Client	Traffic

Name	Log Type
wifi-Top-OS-By-Bandwidth	Traffic
wifi-Top-OS-By-WiFi-Client	Traffic
wifi-Top-SSID-By-Bandwidth	Traffic
wifi-Top-SSID-By-Client	Traffic

Predefined macros

The following table lists the predefined macros for FortiGate.

Name	Description	Category
App Category with Highest Session Count	App Category with Highest Session Count	Traffic
Application with Highest Bandwidth	Application with Highest Bandwidth	Traffic
Application with Highest Session Count	Application with Highest Session Count	Traffic
Attack with Highest Session Count	Attack with Highest Session Count	Attack
Botnet with Highest Session Count	Botnet with Highest Session Count	Traffic
Destination with Highest Bandwidth	Destination with Highest Bandwidth	Traffic
Destination with Highest Session Count	Destination with Highest Session Count	Traffic
Highest Bandwidth Consumed (App Category)	Highest Bandwidth Consumed (App Category)	Traffic
Highest Bandwidth Consumed (Application)	Highest Bandwidth Consumed (Application)	Traffic
Highest Bandwidth Consumed (Destination)	Highest Bandwidth Consumed (Destination)	Traffic
Highest Bandwidth Consumed (P2P Application)	Highest Bandwidth Consumed (P2P Application)	Traffic
Highest Bandwidth Consumed (Source)	Highest Bandwidth Consumed (Source)	Traffic
Highest Bandwidth Consumed (Web Category)	Highest Bandwidth Consumed (Web Category)	Web Filter
Highest Bandwidth Consumed (Website)	Highest Bandwidth Consumed (Website)	Web Filter
Highest Risk Application with Highest Bandwidth	Highest Risk Application with Highest Bandwidth	Traffic

Name	Description	Category
Highest Risk Application with Highest Session Count	Highest Risk Application with Highest Session Count	Traffic
Highest Session Count (App Category)	Highest Session Count (App Category)	Traffic
Highest Session Count (Application)	Highest Session Count (Application)	Traffic
Highest Session Count (Attack)	Highest Session Count (Attack)	Attack
Highest Session Count (Botnet)	Highest Session Count (Botnet)	Traffic
Highest Session Count (Destination)	Highest Session Count (Destination)	Traffic
Highest Session Count (Highest Severity Attack)	Highest Session Count (Highest Severity Attack)	Attack
Highest Session Count (P2P Application)	Highest Session Count (P2P Application)	Traffic
Highest Session Count (Source)	Highest Session Count (Source)	Traffic
Highest Session Count (Virus)	Highest Session Count (Virus)	Traffic
Highest Session Count (Web Category)	Highest Session Count (Web Category)	Web Filter
Highest Session Count (Website)	Highest Session Count (Website)	Web Filter
Highest Severity Attack with Highest Session Count	Highest Severity Attack with Highest Session Count	Attack
P2P Application with Highest Bandwidth	P2P Application with Highest Bandwidth	Traffic
P2P Application with Highest Session Count	P2P Application with Highest Session Count	Traffic
Source with Highest Bandwidth	Source with Highest Bandwidth	Traffic
Source with Highest Session Count	Source with Highest Session Count	Traffic
Total Number of Attacks	Total Number of Attacks	Attack
Total Number of Botnet Events	Total Number of Botnet Events	Traffic
Total Number of Viruses	Total Number of Viruses	Traffic
Virus with Highest Session Count	Virus with Highest Session Count	Traffic
Web Category with Highest Bandwidth	Web Category with Highest Bandwidth	Web Filter
Web Category with Highest Session Count	Web Category with Highest Session Count	Web Filter

Name	Description	Category
Website with Highest Bandwidth	Website with Highest Bandwidth	Web Filter
Website with Highest Session Count	Website with Highest Session Count	Web Filter

FortiMail

Predefined charts

The following table lists the predefined charts for FortiMail.

Name	Description	Category
Average Size of Mails	Average size of mails in FortiMail history	History
History Average Size by Hour	Average size of messages per hour in FortiMail history	History
History Connections per Hour	Number of connections per hour in FortiMail history	History
History Messages per Hour	Number of mails per hour in FortiMail history	History
History Total Size by Hour	Total size of exchanged mails per hour in FortiMail history	History
Number of Mail Connections	Number of mail connections in FortiMail history	History
Number of Mails	Number of mails in FortiMail history	History
Top 20 Access List	Top 20 access list in FortiMail history	History
Top 20 IP Policy	Top 20 IP policy in FortiMail history	History
Top 20 Recipient Policy	Top 20 recipient policy in FortiMail history	History
Top 20 Subjects	Top 20 subjects in FortiMail history	History
Top Classifiers by Hour	Top classifiers by hour in FortiMail history	History
Top Disposition Classifiers	Top disposition classifiers in FortiMail history	History
Top History Client Endpoint	Top 10 clients endpoint in FortiMail history	History

Name	Description	Category
Top History Client IP	Top 10 client IP in FortiMail history	History
Top History Client MSISDN	Top 10 clients MSISDN in FortiMail history	History
Top History Local Recipient	Top 10 local recipients in FortiMail history	History
Top History Local Sender	Top 10 local senders in FortiMail history	History
Top History Local User	Top 10 local users in FortiMail history	History
Top History Local Virus Recipient	Top 10 local virus recipients in FortiMail history	History
Top History Local Virus Sender	Top 10 local virus senders in FortiMail history	History
Top History Mail Dest IP	Top 10 mail destination IP in FortiMail history	History
Top History Recipient	Top 10 recipients in FortiMail history	History
Top History Remote Address	Top 10 remote address in FortiMail history	History
Top History Remote Recipient	Top 10 remote recipients in FortiMail history	History
Top History Remote Sender	Top 10 remote senders in FortiMail history	History
Top History Remote Virus Recipient	Top 10 remote virus recipients in FortiMail history	History
Top History Remote Virus Sender	Top 10 remote virus senders in FortiMail history	History
Top History Sender	Top 10 senders in FortiMail history	History
Top History Sender Endpoint	Top 10 senders Endpoint in FortiMail history	History
Top History Sender IP	Top 10 sender IP in FortiMail history	History
Top History Sender MSISDN	Top 10 senders MSISDN in FortiMail history	History
Top History Total Active EmailAddress	Top 10 total active email address per domain	History
Top History Total Sent Received	Top 10 total sent received in FortiMail history	History
Top History Virus	Top 10 viruses in FortiMail history	History

Name	Description	Category
Top History Virus Dest IP	Top 10 virus destination IP in FortiMail history	History
Top History Virus Endpoint	Top 10 viruses endpoint in FortiMail history	History
Top History Virus IP	Top 10 virus IP in FortiMail history	History
Top History Virus MSISDN	Top 10 viruses MSISDN in FortiMail history	History
Top History Virus Recipient	Top 10 virus recipients in FortiMail history	History
Top History Virus Sender	Top 10 virus senders in FortiMail history	History
Top Spammed Domains	Top spammed domains in FortiMail history	History
Top Spammed Users	Top spammed users in FortiMail history	History
Total Message Delay	Total message delay in FortiMail history	Event
Total Message TransmissionDelay	Total message transmissionDelay in FortiMail history	Event
Total Size of Mails	Total size of mails in FortiMail history	History

Predefined datasets

The following table lists the predefined datasets for FortiMail.

Name	Log Type
fml-Active-EmailAddress-Summary	History
fml-Average-Size-by-Hour	History
fml-Connections-per-Hour	History
fml-history-Average-Size-of-Mails	History
fml-History-Count-Total-Sent-Received	History
fml-history-Number-of-Mail-Connections	History
fml-history-Number-of-Mails	History
fml-history-Top-Access-List	History
fml-history-Top-Classifiers-By-Hour	History

Name	Log Type
fml-History-Top-Client-Endpoint	History
fml-History-Top-Client-IP	History
fml-History-Top-Client-MSISDN	History
fml-history-Top-Disposition-Classifiers	History
fml-history-Top-IP-Policy	History
fml-History-Top-Local-Recipient	History
fml-History-Top-Local-Sender	History
fml-History-Top-Local-User	History
fml-History-Top-Local-Virus-Recipient	History
fml-History-Top-Local-Virus-Sender	History
fml-History-Top-Mail-Dest-IP	History
fml-History-Top-Recipient	History
fml-history-Top-Recipient-Policy	History
fml-History-Top-Remote-Address	History
fml-History-Top-Remote-Recipient	History
fml-History-Top-Remote-Sender	History
fml-History-Top-Remote-Virus-Recipient	History
fml-History-Top-Remote-Virus-Sender	History
fml-History-Top-Sender	History
fml-History-Top-Sender-Endpoint	History
fml-History-Top-Sender-IP	History
fml-History-Top-Sender-MSISDN	History
fml-history-Top-Spammed-Domains	History
fml-history-Top-Spammed-Users	History

Name	Log Type
fml-history-Top-Subjects	History
fml-History-Top-Virus	History
fml-History-Top-Virus-Dest-IP	History
fml-History-Top-Virus-Endpoint	History
fml-History-Top-Virus-IP	History
fml-History-Top-Virus-MSISDN	History
fml-History-Top-Virus-Recipient	History
fml-History-Top-Virus-Sender	History
fml-history-Total-Message-Delay	Event
fml-history-Total-Message-Transmission-Delay	Event
fml-history-Total-Size-of-Mails	History
fml-Messages-per-Hour	History
fml-Total-Size-by-Hour	History

FortiWeb

Predefined charts

The following table lists the predefined charts for FortiWeb.

Name	Description	Category
Top Attack Destinations by Source	Top 10 attacked destinations by source	Attack
Top Attack Destinations by Type	Top 10 attacked destinations by type	Attack
Top Attack Protocols by Type	Top 10 attack protocols by type	Attack
Top Attack Severity by Action	Top 10 detected attack severities by action	Attack
Top Attack Sources	Top 10 sources of attacks	Attack
Top Attack Types	Top 10 detected attack types	Attack

Name	Description	Category
Top Attack Types by Source	Top 10 detected attack types by source	Attack
Top Attack URLs	Top 10 detected attack URLs	Attack
Top Attacked Destinations	Top 10 attacked destinations	Attack
Top Attacked HTTP Methods by Type	Top 10 attacked HTTP methods by attack type	Attack
Top Attacked User Identifications	Top 10 Attacked User identifications	Attack
Top Attacks by Policy	Top 10 attacks used by policies	Attack
Top Event Categories	Top 10 event categories	Event
Top Event Categories by Status	Top 10 event categories by status	Event
Top Event Login by User	Top 10 login events by user	Event
Top Event Types	Top 10 event types	Event
Top Traffic Destinations	Top 10 destinations in FortiWeb traffic	Traffic
Top Traffic Policies	Top 10 policies in FortiWeb traffic	Traffic
Top Traffic Services	Top 10 services in FortiWeb traffic	Traffic
Top Traffic Sources	Top 10 sources in FortiWeb traffic	Traffic

Predefined datasets

The following table lists the predefined datasets for FortiWeb.

Name	Log Type
fwb-attack-Top-Attack-Destinations-By-Source	Attack
fwb-attack-Top-Attack-Destinations-By-Type	Attack
fwb-attack-Top-Attack-Protocols-By-Type	Attack
fwb-attack-Top-Attack-Severities-By-Action	Attack
fwb-attack-Top-Attack-Sources	Attack
fwb-attack-Top-Attack-Types	Attack

Name	Log Type
fwb-attack-Top-Attack-Types-By-Source	Attack
fwb-attack-Top-Attack-URLs	Attack
fwb-attack-Top-Attacked-Destinations	Attack
fwb-attack-Top-Attacked-Http-Methods-By-Type	Attack
fwb-attack-Top-Attacked-User-Identifications	Attack
fwb-attack-Top-Attacks-By-Policy	Attack
fwb-event-Top-event-categories	Event
fwb-event-Top-Event-Categories-By-Status	Event
fwb-event-Top-event-types	Event
fwb-event-Top-login-by-user	Event
fwb-traffic-Top-Destinations	Traffic
fwb-traffic-Top-Policies	Traffic
fwb-traffic-Top-Services	Traffic
fwb-traffic-Top-Sources	Traffic

FortiCache

Predefined charts

The following table lists the predefined charts for FortiCache.

Name	Description	Category
Top 20 Websites by Bandwidth Savings	Top 20 Websites by Bandwidth Savings	Traffic
Top 20 Websites by Cache Rate	Top 20 Websites by Cache Rate	Traffic
Top 20 Websites by Response Time Improvement	Top 20 Websites by Response Time Improvement	Traffic

Predefined datasets

The following table lists the predefined datasets for FortiCache.

Name	Log Type
fch-Top-Websites-by-Bandwidth-Savings	Traffic
fch-Top-Websites-by-Cache-Rate	Traffic
fch-Top-Webistes-by-Response-Time-Improvement	Traffic