FortiManager v4.0 MR3 Patch Release 8
Administration Guide

FortiManager v4.0 MR3 Patch Release 8 Administration Guide

November 25, 2013

02-438-167503-20131125

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

Table of Contents

Table of Figures **13**
Change Log **17**
Introduction **18**
About this document 18
FortiManager documentation 20
What's New in v4.0 MR3 ..... **21**
Global policy improvements 21
Global policy license change 21
Assigning global policies to ADOMs 21
Add global zone to global policy 21
Section view for global and ADOM policy packages 21
Administrative Domain (ADOM) 22
ADOM backup and revision control 22
Install wizard/Import wizard 22
Add device wizard, fast forward support 22
Import policy 22
Virtual Domain (VDOM) 23
Policy usability 23
Multiple policy edit 23
FortiToken support 23
Management model 24
FortiManager VM licensing changes 24
Web-based Manager changes 24
User workspaces 25
Search improvements 25
Improvements to Device Manager 25
Firewall Policies Consistency Check 25
Java Client for Windows 25
IPv6 support 26
Audit logging 26
FortiGate to FortiManager protocol 26
FortiMail support 26
High Availability improvements 26
SNMPv3 support added 26
Additional XML API extensions 26

Fortinet Management Theory 27
Key features of the FortiManager system 27
Configuration revision control and tracking 27
Centralized management 27
Administrative Domains 27
Local FortiGuard service provisioning 27
Firmware management 27
Scripting 28
FortiClient management 28
Fortinet device lifecycle management 28
Inside the FortiManager system 29
Inside the FortiManager management module 30
Using the Web-based Manager 32
System requirements 32
Connecting to the Web-based Manager 32
Web-based Manager overview 33
Viewing the Web-based Manager 33
Using the main toolbar 34
Using the toolbar 34
Using the navigation pane 34
Configuring Web-based Manager settings 35
Changing the Web-based Manager language 35
Changing administrative access to your FortiManager system 36
Changing the Web-based Manager idle timeout 36
Reboot and shutdown of the FortiManager unit 37
Administrative Domains 38
Enabling and disabling the ADOM feature 39
About ADOM modes 40
Switching between ADOMs 40
Normal mode ADOMs 40
Backup mode ADOMs 40
Managing ADOMs 41
Concurrent ADOM access 42
Adding an ADOM 42
Deleting an ADOM 44
Assigning devices to an ADOM 44
Assigning administrators to an ADOM 45
Viewing ADOM assignments 45
Viewing ADOM properties 46

System Settings **48**
Viewing the system status 49
Customizing the dashboard 50
Viewing system information 52
Viewing system resource information 53
Viewing the device summary 55
Viewing license information 55
Viewing unit operation 55
Viewing RAID status 56
Viewing alert messages 58
Using the CLI console widget 59
Configuring general settings 60
Changing the host name 61
Configuring the system time 61
Updating the system firmware 63
Backing up and restoring the system 64
Configuring RAID 67
Configuring network settings 70
Managing certificates 74
Configuring High Availability 76
Managing administrators 78
Monitoring administrator sessions 78
Configuring administrator accounts 79
Managing administrator access 83
Managing remote authentication servers 87
Configuring global admin settings 93
Managing FortiGuard Services 94
Configuring FortiGuard services 95
Configuring FortiGuard updates 96
Managing firmware images 97
Viewing local event logs 97
Configuring advanced settings 98
Configuring SNMP 98
Configuring metadata requirements 105
Configuring advanced settings 108
Alerts 109
Device Log 114
Using FortiManager Wizards **116**
Using the add device wizard 116
Launching the add device wizard 116
Importing a device 119
Adding a Device 123

Using the install wizard 127
Launching the install wizard 127
Installing a policy package 128
Installing device settings 131
Overview of the add device wizard 133
Device Management 135
Device manager overview 135
Viewing device summaries 135
Viewing managed devices 135
Viewing a single device 137
Using list filters 140
Managing devices 141
Adding a device 142
Replacing a managed device 142
Deleting a device 143
Editing device information 143
Refreshing a device 144
Importing policies to a device 145
Importing and exporting devices 145
Setting unregistered device options 150
Configuring devices 150
Configuring a device 150
Configuring virtual domains (VDOMs) 151
Working with device groups 155
Adding a device group 155
Deleting a device group 156
Editing device group information 156
Viewing the device group summary 156
Managing FortiGate chassis devices 157
Viewing chassis dashboard 160
Using the CLI console for managed devices 163
Policies and Objects 165
About policies 165
Policy theory 167
Policy workflow 168
Provisioning new devices 168
Day-to-day management of devices 168
Managing policy packages 169
Create a new policy package or folder 169
Remove a policy package or folder 169
Rename a policy package or folder 170
Install a policy package 170
Perform a policy consistency check 170
About objects and dynamic objects 172

Managing objects and dynamic objects 173
Create a new object or group 173
Map the dynamic object 174
Remove an object or group 174
Edit an object or group 174
Clone an object or group 174
Search where an object or group is used 175
Search objects 175
FortiToken configuration example 176
VPN Console 177
Configuring a VPN 178
Enable or disable VPN consoles 178
Create a firewall address 178
Create a VPN configuration 178
Add a VPN gateway 183
Create VPN firewall policies 185
Installing Device Configurations 186
Checking device configuration status 186
Managing configuration revision history 187
Downloading and importing a configuration file 189
Comparing different configuration files 189
Advanced Features 191
About global policies and objects 191
Assigning global policies to ADOMs 192
Searching for global objects content 192
IP address search rules 193
Configuring web portals 197
Creating a web portal 198
Configuring the web portal profile 199
Creating a portal user account 203
External users 203
Using the web portal 204
Application Program Interfaces 205
XML API 205
Connecting to FortiManager web services 205
Fortinet developer network 206
Java-based Administration Client 207
System requirements 207
Installing and logging in to the Java-based client 207
Java-based manager overview 208
Using the main toolbar 209
Using the navigation pane 209
Using the content pane 210

Java-based manager features 210
Drag and drop 210
Tabs 211
Improved adding and editing windows 211
Working with Scripts 213
Device view 213
Individual device view 214
Scheduling a script 215
Script view 216
Creating or editing a script 218
Cloning a script 219
Exporting a script 220
Script samples 220
CLI scripts 220
TCL scripts 225
FortiGuard Services 242
FortiGuard center 243
Connecting the built-in FDS to the FDN 248
Configuring devices to use the built-in FDS 249
Matching port settings 249
Handling connection attempts from unregistered devices 250
Configuring FortiGuard services in the FortiGuard Center 250
Enabling push updates 250
Enabling updates through a web proxy 251
Overriding default IP addresses and ports 252
Scheduling updates 252
Accessing public FortiGuard web filtering and email filtering servers 253
Viewing FortiGuard services from devices and groups 256
FortiGuard Antivirus and IPS Statistics for a device 256
Web filter category detail 257
FortiGuard web filter and email filter statistics 257
License information 257
Device History 260
Logging events related to FortiGuard services 260
Logging FortiGuard Antivirus and IPS updates 260
Logging FortiGuard Web Filtering or Email Filter events 261
Viewing service update log events 262
Restoring the URL or antispam database 263
Firmware and Revision Control 264
Viewing a device or group's firmware 264
Downloading firmware images 267
Installing firmware images 269

Real-time Monitor **270**
RTM monitoring 270
RTM Dashboards 271
FortiManager system alerts 274
Alerts event 274
Configuring alerts 276
Alert console 281
Device log 282
Device log setting 282
Device log access 284
FortiClient Manager **285**
FortiClient Manager maximum managed agents 285
About FortiClient Manager clustering 286
FortiClient Manager window 286
Main menu bar 287
Navigation pane 288
Client group tree 290
FortiClient menu 290
Message center 290
Dashboard 290
Management event 291
Client alert 293
Working with clients (FortiClient agents) 295
Viewing the clients lists 295
Filtering the clients list 297
Searching for FortiClient agents 297
Adding or removing temporary clients 298
Removing or relicensing unlicensed clients 299
Deploying licenses to standard edition clients 300
Deleting FortiClient agents 300
Working with FortiClient groups 301
Overview of client groups 301
Viewing FortiClient groups 302
Adding a FortiClient agent group 302
Deleting a FortiClient agent group 303
Editing a FortiClient agent group 304
Viewing group summaries 304
Configuring settings for client groups 304
Managing client configurations and software 306
Deploying FortiClient agent configurations 306
Retrieving a FortiClient agent configuration 306
Working with FortiClient software upgrades 307
FortiClient license keys 308

Working with web filter profiles 309
About web filtering 309
Viewing and editing web filter profiles 310
Configuring a web filter profile 310
Configuring FortiClient manager system settings 310
Configuring FortiClient manager clustering 311
Configuring FortiClient manager cluster members 312
Configuring email alerts 312
Configuring LDAP for web filtering 313
Configuring LDAP settings 314
Configuring an LDAP server 314
Working with Windows AD users and groups 315
Active Directory Organizational Units grouping 316
Configuring FortiClient group-based administration 318
Assigning group administrators 318
Configuring enterprise license management 319
Configuring an enterprise license 319
Creating a customized FortiClient installer 320

Configuring FortiClient agent settings 321
Viewing system status of a FortiClient agent 321
Configuring system settings of a FortiClient agent 323
Adding trusted FortiManager units to a FortiClient agent 325
Managing pending actions for a FortiClient agent 326
Configuring the log settings of a FortiClient agent 327
Configuring lockdown settings 328
Configuring the VPN settings of a FortiClient agent 328
Configuring a VPN security policy on a FortiClient agent 329
Configuring VPN options of a FortiClient agent 329
Configuring WAN Optimization settings of a FortiClient agent 330
Configuring antivirus settings on a FortiClient agent 331
Antivirus scans 332
Configuring antivirus options 333
Viewing the firewall monitor of a FortiClient agent 338
Creating firewall policies on a FortiClient agent 340
Configuring firewall addresses on a FortiClient agent 341
Configuring firewall address groups on a FortiClient agent 342
Defining firewall applications on a FortiClient agent 343
Defining firewall protocols on a FortiClient agent 344
Configuring firewall protocol groups on a FortiClient agent 345
Configuring firewall schedules on a FortiClient agent 346
Configuring firewall schedule groups 347
Configuring trusted IPs exempted from intrusion detection 347
Configuring ping servers for a FortiClient agent firewall 348
Setting the firewall options of a FortiClient agent 348
Selecting a web filter profile for a FortiClient agent 351
Configuring web filter options on a FortiClient agent 352
Configuring Email Filter settings on a FortiClient agent 353
Configuring Email Filter options 354
Configuring anti-leak options on a FortiClient agent 355
High Availability 356
HA overview 356
Synchronizing the FortiManager configuration and HA heartbeat 357
If the primary unit or a backup unit fails 357
FortiManager HA cluster startup steps 358
Configuring HA options 358
General FortiManager HA configuration steps 360
Web-based Manager configuration steps 361
Monitoring HA status 363
Upgrading the FortiManager firmware for an operating cluster 363
FortiManager Firmware 365
Upgrade information 365

Upgrading from FortiManager v4.0 MR3 366
Step 1: Backup FortiManager database and configuration 366
Step 2: Transfer the firmware image to FortiManager 366
Step 3: Verify the upgrade 366
Step 4: Upgrade FortiOS devices 366
Upgrading from FortiManager v4.0 MR2 367
Step 1: Prepare FortiManager for upgrade 367
Step 2: Backup the database and transfer the firmware image 367
Step 3: Verify the upgrade 367
Step 4: Populate policy and objects with the import wizard 369
Downgrading FortiManager 370
Appendix A: Maximum Values/Features 371
Appendix B: FortiManager VM 372
FortiManager VM system requirements 372
FortiManager VM licence enhancements 372
Index 373

Table of Figures

FortiManager conceptual diagram 29
Management module 30
Default FortiManager Configuration window 33
Main toolbar 34
Unit operation actions in the Web-based Manager 37
Enabling ADOMs 39
Backup mode ADOM device revision history 41
ADOM table 41
Add an ADOM 43
ADOM dashboard example 46
FortiManager system dashboard 49
Adding a widget 50
A minimized widget 51
System information widget 52
System resources widget (Real time display) 53
System resource widget (Historical display) 53
Edit system resources settings window 54
Device Summary widget 55
VM license information widget 55
Unit operation widget 56
RAID monitor displaying a RAID array without any failures 56
Alert message console widget 58
List of all alert messages 59
CLI console widget 60
Edit host name dialog box 61
Time settings dialog box 62
Firmware upgrade dialog box 63
Backup dialog box 65
All settings configuration restore dialog box 66
RAID settings dialog box 67
Network screen 70
Network interface list 71
Configure network interfaces 72
Routing table 73
Create new route 73
Local certificates window 74
Local certificate detail window 75
Cluster settings dialog box 76
Administrator session list 78
Administrator list 79
Creating a new administrator account 80
Editing an administrator account 82
Administrator profile list 84
Create new profile dialog box 85
Edit administrator profile window 86
RADIUS server list 88
New RADIUS server window 88

LDAP server list 90
New LDAP server dialog box 90
New TACACS+ server dialog box 92
Administrative settings dialog box 93
FortiGuard center dialog box 95
Server settings dialog box 96
Firmware images list 97
SNMP configuration 99
FortiManager SNMP community 101
System objects metadata 106
Add meta-field (system object) 106
Config objects metadata 107
Add meta-field (config object) 108
Advanced settings 108
Alert event window 109
Create new alert event window 110
Mail server window 111
Mail server settings 112
Syslog server window 112
Syslog server settings 112
Alert message console window 113
Alert console settings 113
Log setting window 114
Add Device icon 116
Add device wizard login window 117
Import device summary window 117
Discover method summary window 118
Add model device method window 118
Importing device additional information window 119
Zone map window 120
Import policy summary 121
Import object summary 121
Device import successful window 122
Import device summary window 123
Adding device additional information window 123
Adding device model additional information window 124
Confirmation of success or failure 125
Zone map window 126
Add device summary window 126
Add model device summary window 127
Install icon 127
Install policy package 128
Policy package device selection window 128
Policy package zone validation window 129
Policy package policy validation window 129
Policy package installation window 130
Device installation history 130
Install device settings only 131
Device settings device selection window 131
Device settings successful installation window 132
Device settings failed installation window 132
Device installation history 133

Device manager device list layout 135
Right click menu options 136
Example FortiGate unit summary 138
Device filter settings dialog box 140
Device filter settings dialog box 141
Device filter settings dialog box 141
Edit device 143
Device manager right-click menu 144
Create new virtual domain 152
Adding a group 155
Device group summary screen 157
Enable chassis management 158
Add new chassis 159
CLI console 164
Management module 166
Policy window 166
Create new policy package 169
Enter new policy package details 169
Edit policy package dialog box 170
Consistency Check dialog box 171
Policy Check dialog box 171
Consistency check results window 172
Managing objects and dynamic objects 172
Example object table 173
Creating a new Firewall object address 173
Map dynamic address 174
Where Used dialog box 175
Search objects dialog box 176
New local user window 176
VPN list 177
Create VPN window 179
Add VPN Managed Gateway dialog box 183
Add VPN External Gateway dialog box 184
Configuration and Installation Status widget 186
Revision history tab 187
Add a tag to a configuration version 188
Revision Diff window 190
License information widget 191
Web Portal Window 199
Add profile dialog box 199
Blank web portal window 200
Adding web portal content 200
Logo Preferences 202
Portal properties window 202
Add User window 203
Add External User window 204
Java-based administration client login screen 207
Java-based administration client main window 208
Default main menu bar 209
Java-based manager content pane 210
Reorganizing tabs in the Java-based administration client 211
Policy editor widow 212

Individual device view 214
Scheduling a script 215
CLI script repository 216
Create or edit a script 218
Cloning a script 219
Enable FortiGuard settings 244
FortiGuard Antivirus and IPS Settings 246
Overriding FortiGuard Server 253
Manually uploading AV or IPS updates 255
Device group service usage: license Information 258
Firmware Information (device) 265
Firmware Information (group) 265
Firmware Images 267
Upload Firmware Image dialog box 269
Example RTM Dashboards 271
Rename a dashboard 272
Reset a dashboard 273
Add Monitor window 273
Viewing alert events 274
Adding alert events 275
Mail server list 277
Adding mail servers 277
SNMP access list 278
Adding a SNMP community 280
Syslog server list 281
Adding syslog Server 281
Alert message console 282
Device Log Setting 283
Device Log Access 284
FortiClient manager 287
Example of how FortiClient Manager determines the group names for OU groups. 317
Cluster Settings 359
FortiManager HA status 363
Right click to create 368
Right-click target device and select Import Config 369
Import Wizard 369

Change Log

Date	Change Description
2012-04-06	Initial release
2012-04-12	Updated chassis management, under devices chapter. Updated *Advanced Settings* section.
2012-06-08	Removed references to device locks.
2012-06-18	Revised section on ADOM locking.
2012-07-16	Added Appendix A FortiManager Maximum Values. Added Map Dynamic Object note under Policies and Objects section.
2012-09-03	Updated document template.
2012-09-12	Removed command `set verify_serial_number enable`.
2012-12-12	Modified compatible Internet browsers.
2013-01-21	Updated HA configuration chapter.
2013-01-29	Updated HA cluster upgrade instructions.
2013-01-31	Updated number of peers in an HA cluster to four.
2013-02-22	Updated for FortiManager v4.0 MR3 Patch Release 7. Removed references to the global policy license. FortiManager v4.0 MR3 Patch Release 7 or later supports global policy without a license.
2013-11-25	Updated for FortiManager v4.0 MR3 Patch Release 8.

Introduction

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

Using the FortiManager system, you can:

- configure multiple FortiGate units (including FortiGate, FortiWiFi, FortiGate-One, FortiGate VM), FortiCarrier units, FortiMail units, FortiSwitch units, and FortiClient endpoint security agents,
- segregate management of large deployments easily and securely by grouping devices and agents into geographic or functional administrative domains (ADOMs),
- configure and manage VPN policies,
- monitor the status of these units,
- view device logs,
- update the antivirus and attack signatures,
- provide web filtering and email filtering service to the licensed devices as a local FortiGuard Distribution Network (FDN) server.
- update the firmware images of the devices.

The FortiManager system scales to manage up to 10000 devices and virtual domains (VDOMS) and up to 120000 FortiClient agents from a single FortiManager interface. It is designed for medium to large enterprises and managed security service providers. FortiManager system architecture emphasizes reliability, scalability, ease of use, and easy integration with third-party systems.

This section contains the following topics:

- About this document
- FortiManager documentation

About this document

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

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

This document contains the following information:

- What's New in v4.0 MR3 lists and describes some of the new features and changes in FortiManager v4.0 MR3 and Patch Releases 1 to 8.
- Fortinet Management Theory describes key features of the FortiManager system.
- Using the Web-based Manager introduces the FortiManager Web-based Manager interface that is used to manage and configure supported Fortinet units and FortiClient agents, and to view FortiGate unit configuration, device status, system health, real time logs, and historical logs.

- Administrative Domains (ADOMs) describes ADOMs that can define sets of devices to be controlled by one or more administrators.
- System Settings describes how to control and monitor the operation of the FortiManager system, including network settings, managing firmware revisions, configuration backup and administrator access.
- Using FortiManager Wizards describes how to use the Install, Add Device, and Import Device wizards.
- Device Management describes adding, configuring and managing devices, Virtual Domains (VDOMs) and working with device groups.
- Policies and Objects describes policy workflow, provisioning, policy packages, objects and dynamic objects.
- VPN Console describes how to configure a VPN and firewall policies.
- Installing Device Configurations describes installing configuration changes to the devices and pulling the existing configurations from the devices.
- Advanced Features describes administrative web portals and portal access.
- Application Program Interfaces
- Java-based Administration Client introduces the FortiManager java-based administration client tool that can used to manage and configure supported devices and FortiClient agents.
- Working with Scripts describes how to create and manage scripts from devices that are in operation. Administrators can use functions, such as the configure function, the debug function, the show function, and the get function, to manage devices using scripts.
- FortiGuard Services describes how to use the FortiManager system as a local update server for AV and IPS signatures and a on-site FDN server for FortiGuard Web Filtering and Email Filter services.
- Firmware and Revision Control describes how to view, download and install device firmware images.
- Real-time Monitor describes how to monitor the status of a number of devices, system alerts and device log.
- FortiClient Manager describes how to use the FortiClient Manager to centrally manage FortiClient agents.
- High Availability describes how to configure and manage a FortiManager high availability clusters.
- FortiManager Firmware

FortiManager documentation

The following FortiManager product documentation is available:

- *FortiManager v4.0 MR3 Patch Release 8 Administration Guide*

  This document describes how to set up the FortiManager system and use it to manage supported Fortinet units and FortiClient agents. It includes information on how to configure multiple Fortinet units and FortiClient agents, 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 filtering service to the licensed FortiGate units as a local FortiGuard Distribution Network (FDN) server, firmware revision control and updating the firmware images of the managed units and agents.

- *FortiManager System QuickStart Guide*

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

- *FortiManager online help*

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

- *FortiManager v4.0 MR3 Patch Release 8 CLI Reference*

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

- *FortiManager v4.0 MR3 Patch Release 8 Release Notes*

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

- *FortiManager v4.0 MR3 Patch Release 8 Log Message Reference Guide*

  The FortiManager Log Message Reference Guide describes the structure of FortiManager log messages and provides information about the log messages that are generated by the FortiManager system.

What's New in v4.0 MR3

This chapter lists and describes some of the key changes and new features added to the FortiManager system.

This document was written for FortiManager v4.0 MR3 Patch Release 8.

Global policy improvements

Global policy license change

FortiManager v4.0 MR3 Patch Release 8 supports the global policy feature without a license.

Assigning global policies to ADOMs

FortiManager v4.0 MR3 allows you to specify which policy package within each ADOM, will inherit the global policy or global database. This enhancement provides a finer granularity to assign specific policy packages within each ADOM.

Add global zone to global policy

FortiManager v4.0 MR3 adds a global zone objects menu and table for adding global zones to global policies. The following changes are included:

- Within an ADOM, the global zones are read-only and can not be deleted or edited in the Objects database.
- You will need to populate the global zones with interfaces from each device manager.
- Global zones can be used for both global level policy packages as well as ADOM level policy packages, after it is assigned from global to the specified ADOM.

Section view for global and ADOM policy packages

FortiManager v4.0 MR3 improves the section view menu, by zone with custom label sections. This change adds the following features:

- View with global sections or with zone sections with custom labels
- Option to toggle between views
- Support for both ADOM and global policy packages.

Administrative Domain (ADOM)

The following improvements have been made to the ADOM list page:

- When the global admin user logs in, they are directed to the ADOM list page.
- When selecting the ADOM name, the left menu item will be selected and the ADOM dashboard will be displayed.
- The right-click context menu has a new option to enter the ADOM.
- A search field has been added to the navigation pane to quickly search for a specific ADOM.
- If backup mode has been configured, backup is displayed beside the ADOM name in the column.
- A new column has been added to show if the ADOM has any alerts and a count of the number of alerts.
- A status icon is displayed beside each device to show if communication is up or down.
- When you hover the mouse pointer over an ADOM, an *Enter* dialogue box appears. Left-click *Enter* to enter the ADOM menu.

ADOM backup and revision control

FortiManager v4.0 MR3 introduced two administrative domain (ADOM) configuration modes: *Normal* and *Backup*. FortiManager v4.0 MR3 also introduces improvements with how the FortiManager handles backup and revision control in both these modes of operation. See "Administrative Domains" on page 38 for more information.

Install wizard/Import wizard

FortiManager v4.0 MR3 provides enhancements to the install wizard and import wizard. These changes include:

- Clear description of error messages
- Preview option to view the installation changes for a policy package
- Preview option for device settings installation

Add device wizard, fast forward support

An option has been added to device discovery that allows you to ignore prompts when adding or importing a device unless errors occur. If the device has VDOMs, this option is hidden on the discovery page and displayed on the VDOM page.

Import policy

FortiManager v4.0 MR3 provides enhancements to the import policy wizard which allows you to select specific policies to import. This granularity provides you with more control over the device and policy import process. Both IPv4 and IPv6 policies are supported.

Virtual Domain (VDOM)

FortiManager v4.0 MR3 provides the following improvements to the import wizard and device management to handle the import of multiple VDOMs and import of devices/VDOMs when upgrading or moving devices between ADOMS:

- New add VDOM page in the import wizard.
- If the device has VDOMs enabled with more than one VDOM, the add VDOM page will be displayed.
- The first VDOM will be selected by default, as each VDOM is imported, it will be greyed out in the list.
- You can specify a specific VDOM to import
- You can select the *Import All* checkbox to automatically import all VDOMs, or any remaining VDOMs that have not been imported.
- You can choose the *Skip Remaining* button to ignore any remaining VDOMs and jump straight to the summary page.

Once a VDOM is added, you will return to the *Add VDOM* page.

Policy usability

FortiManager v4.0 MR3 adds a *Set Profile* option in the right-click menu on the policy page. You can use option to assign a new profile to the firewall policy without having to remove and re-add the profile or open the edit policy page.

Multiple policy edit

FortiManager v4.0 MR3 provides an enhancement to allow you to select multiple policies and then right-click to modify the UTM settings for all the selected policies.

FortiToken support

FortiManager v4.0 MR3 provides FortiToken support as a configurable object. See “FortiToken configuration example” on page 176.

Management model

The FortiManager system in v4.0 MR3 has been changed from what you may be used to from earlier versions. In previous versions there were two modes of operation: EMS and GMS. In v4.0 MR3, these have been combined into a single, united workflow that is suitable for users of either mode.

The new management model has the following configuration management components per ADOM:

- *Policy & Objects*
- *Real-Time Monitor*
- *FortiClient Manager*
- *Add Device Wizard*
- *Install Wizard*
- *Device Settings Management*:
  - *Device Summary & Status*
  - *VDOM Synchronization*
  - *Web-based Manager Scripts*

For more information on the new management model, see "Fortinet Management Theory" on page 27.

FortiManager VM licensing changes

With FortiManager v4.0 MR3 the following changes have been made to FMG-VM:

- Automatic fifteen (15) day evaluation license
- Removal of requirement to have FMG-VM contact FortiGuard Distribution Servers (FDS) for license activation
- Stackable license model for FMG-VM license add-ons
- License can be applied through the FMG-VM CLI.

See "FortiManager VM" on page 372.

Web-based Manager changes

FortiManager v4.0 MR3 includes a number of changes to the Web-based Manager:

- Tab Bar

  The Web-based Manager now features a tab bar to improve its organization and simplify access to important system functions.
- System Settings

  The *System* menu in the Web-based Manager has been improved to make it easier to use. Improved support for widgets has been added.
- Installation improvements

  FortiManager v4.0 MR3 simplifies installation of updates to managed devices, allowing "1-click" installation of updates.
- Policy table improvements

  The policy table has had several improvements made, including contextual menus, to improve usability.

User workspaces

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

For further reading on how all the new changes to the Web-based Manager work, please refer to "Concurrent ADOM access" on page 42.

Search improvements

Searching in FortiManager v4.0 MR3 has been updated to allow users to find the information they are looking for easier. This includes global object searches, plus the ability to easily locate where objects are being used in specific policy packages with the *Where Used* feature.

Improvements to Device Manager

FortiManager v4.0 MR3 adds many usability improvements to the *Add Device* tab, including:

- New layout design
- The process for adding, importing, and installing devices has been streamlined with the Add Device and Install wizards
- Real-time progress monitoring
- Real-time FortiGate data.

For more information on *Device Manager*, please refer to "Device Management" on page 135.

Firewall Policies Consistency Check

FortiManager v4.0 MR3 adds the ability to check all firewall rules and policies to ensure consistency and eliminate rule conflicts that may prevent your devices from passing traffic. The check will verify:

- Object duplication: two objects that have identical definitions
- Object shadowing: one object completely shadows 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.

This will allow you to optimize your rule and policy sets and potentially reduce the size of your databases.

For more information, see "Perform a policy consistency check" on page 170.

Java Client for Windows

FortiManager v4.0 MR3 now supports a Java-based desktop client for Microsoft Windows that allows an administrator to interact with FortiManager via their desktop. For users with large data sets, this can assist in easier and faster management of their networks.

Please see "Java-based Administration Client" on page 207.

IPv6 support

FortiManager v4.0 MR3 now fully supports all FortiGate IPv6 features, both via the CLI and the Web-based Manager.

Audit logging

FortiManager v4.0 MR3 now provides full logging of all administrative activities.

FortiGate to FortiManager protocol

There have been revisions to the FGFM protocol used to communicate between FortiGate and FortiManager devices, including the ability to remotely execute commands on remote FortiGate devices.

FortiMail support

FortiManager v4.0 MR3 now supports remote managing of FortiMail devices. FortiManager is now able to discover and add FortiMail devices; remotely monitor FortiMail status; view, edit, install and backup FortiMail settings and configuration files; and remotely create, view, edit, delete and execute scripts.

High Availability improvements

FortiManager v4.0 MR3 brings improvements to HA mode:

- Automatic firmware updating to slave units when the primary unit is upgraded
- Automatic removal of inoperable slave units, with notification to the administrator indicating that action is required
- Improved uptime and availability enhancements.

Please review the *High Availability* section of this document, located on page 356 for further information.

SNMPv3 support added

FortiManager v4.0 MR3 now has SNMPv3 support, allowing SNMPv3 queries, replies, authentication and views. More information on this feature is available in the *FortiManager v4.0 MR3 Patch Release 7 CLI Reference*, available online at http://docs.fortinet.com/.

Additional XML API extensions

FortiManager v4.0 MR3 adds additional extensions to the XML definition to allow better group management.

Fortinet Management Theory

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

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

The FortiManager a scales to manage up to 10000 devices and virtual domains (VDOMs) and up to 120000 FortiClient agents 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 and agent 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 and agents into geographic or functional administrative domains (ADOMs).

Local FortiGuard service provisioning

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

Firmware management

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

Scripting

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

FortiClient management

FortiManager can also be used to manage, monitor and update your FortiClient endpoint security agents.

Fortinet device lifecycle management

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

- 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

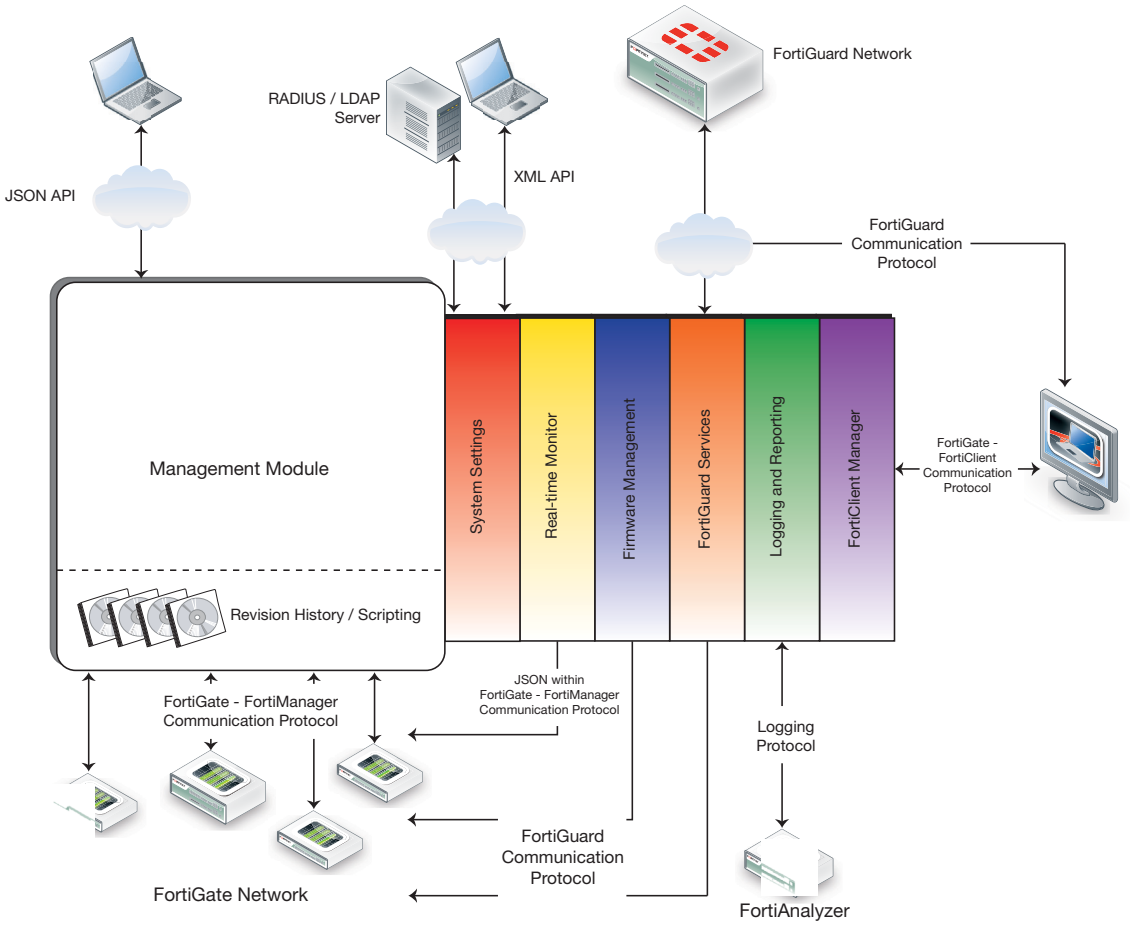
  The administrator performs configuration updates as needed to keep devices up-to-date.
- Upgrading

  Virus definitions, attack and data leak prevention signatures, web and spam filtering services as well as device firmware images, are all kept current to provide continuous protection for devices in the security infrastructure.

Inside the FortiManager system

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

Figure 1: FortiManager conceptual diagram



Management module

The management module contains all of your header and footer policies that are applicable to all ADOMs, your individual Administration Domains, all policy folders, objects and configuration revisions. This is also where the FortiManager sends updates to managed devices. See “Inside the FortiManager management module” for more details.

System settings

The systems settings tab enables the configuration of system settings and monitors the operation of your FortiManager unit.

Real-time monitor

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

FortiGuard services

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

Logging and reporting

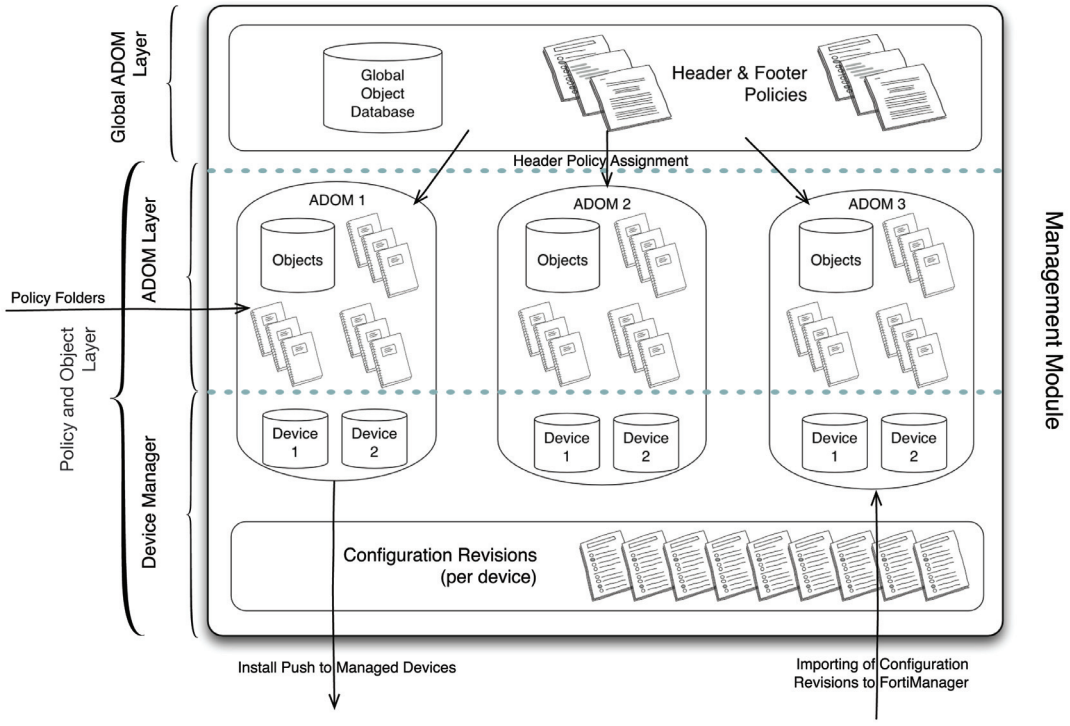
The logging and reporting tab provides detailed logging information which can be exported and viewed.

FortiClient manager

The FortiClient manager tab can be used to centrally manage FortiClient endpoint security agents. This feature allows administrators to update and manage FortiClient agents from within the FortiClient manager tab.

Inside the FortiManager management module

Figure 2: Management module



Global ADOM layer

The Global ADOM layer contains two key pieces: the Global Object Database and all Header and Footer Policies.

- Global Object Database
- 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.

For more information on the Global ADOM Layer feature, refer to "Advanced Features" on page 191.

ADOM layer

The ADOM layer is where the FortiManager manages individual devices or groups of devices. It is inside this layer where policy tables and folders are created and 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, IPS information, AV definitions, and Web Filtering and email filtering.

Device manager layer

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

Using the Web-based Manager

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

This section includes the following topics:

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

System requirements

The following web browsers are supported by FortiManager v4.0 MR3 Patch Release 8:

- Microsoft Internet Explorer versions 9 and 10
- Mozilla Firefox versions 24 and 25
- Google Chrome version 31

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

To minimize scrolling, the computer's screen should have a resolution that is a minimum of 1280 x 1024 pixels.

Connecting to the Web-based Manager

The Web-based Manager can be accessed by URL using the network interfaces' enabled administrative access protocols and IP addresses.

By default, the URL when accessing the Web-based Manager through port1 is https://192.168.1.99/.

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. In that case, for the URL, use either a DNS-resolvable domain name for the Fortinet unit, or the IP address that you configured for the network interface to which you are connected.

For example, you might have configured port2 with the IP address 10.0.0.1 and enabled HTTPS. You might have also configured a private DNS server on your network to resolve fortimanager.example.com to 10.0.0.1. To access the Web-based Manager through port2, you could enter either https://fortimanager.example.com/ or https://10.0.0.1/.

For information on enabling administrative access protocols and configuring IP addresses, see "Configuring network interfaces" on page 72.

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

Web-based Manager overview

The four main parts of the FortiManager Web-based Manager are the main menu bar, the tab bar, the navigation pane, and the content pane. You can use the Web-based Manager menus, lists, and configuration pages to configure most FortiManager settings. Configuration changes made using the Web-based Manager take effect immediately without resetting the FortiManager system or interrupting service.

The Web-based Manager also includes detailed online help. Selecting *Help* on the main menu bar displays help for the current Web-based Manager tab.

The navigation pane and content pane information displayed to an administrator vary according to the administrator account settings and access profile that have be configured for that user. The system settings tab, for example, is available only when you log in as the default `admin` administrator. This administrator has full (super-user) privileges and is allowed to access and configure any part of the FortiManager system and its managed devices. For more information about administrator accounts and their privileges, see "Managing administrators" on page 78.

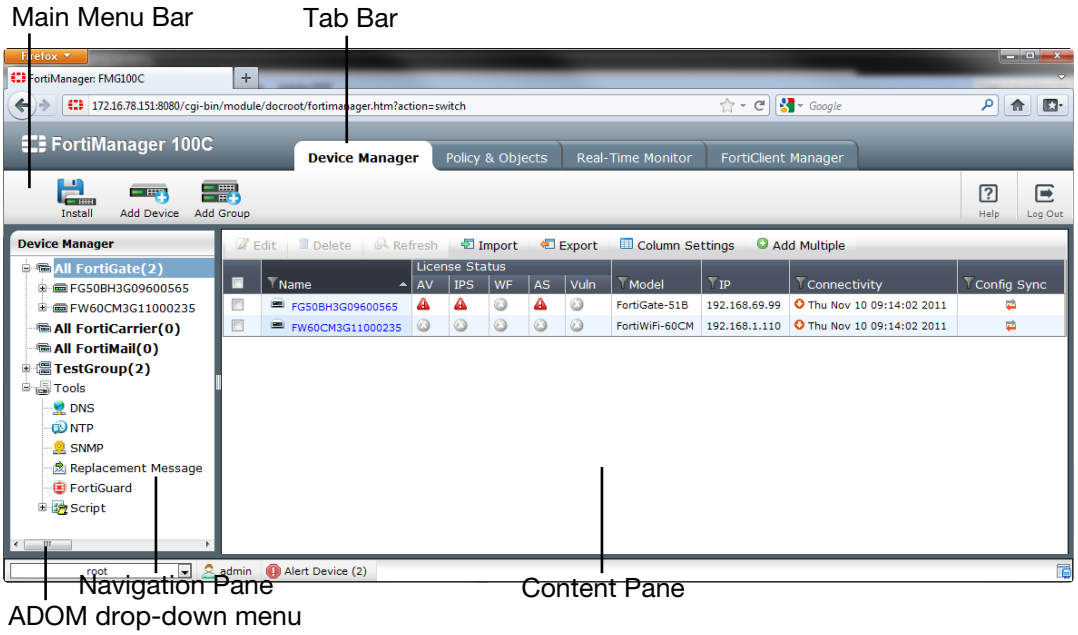
When you log in to the FortiManager unit as the `admin` administrator, the Web-based Manager opens to the *System Settings* menu and displays the system dashboard. From this menu you can monitor the system status and perform various system administration tasks. For more information about using the System Settings menu, see "System Settings" on page 48.

This section describes the following topics:

- Using the main toolbar
- Using the toolbar
- Using the navigation pane

Viewing the Web-based Manager

Figure 3: Default FortiManager Configuration window



The illustration above shows the FortiManager Web-based Manager default screen. The four main parts of the FortiManager Web-based Manager are the main menu bar, the tab bar, the navigation pane, and the content pane. Use the Web-based Manager menus, lists, and configuration pages to configure most FortiManager settings. Configuration changes made

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

Using the main toolbar

At the top of the FortiManager system display is the main toolbar, which includes icons for many common tasks. The following icons are available:

Figure 4: Main toolbar

Using the toolbar

Install	Select to install changes from the FortiManager database to the physical devices. Optionally install to FortiGate or FortiCarrier units. See “Installing Device Configurations” on page 186.
Add Device	Select to add a FortiGate, FortiSwitch FortiCarrier, or FortiMail unit to the current administration domain. See “Adding a device” on page 142.
Add Group	Select to add a group of FortiGate devices to the current administration domain. See “Adding a device” on page 142
Help	Select to view the online help for the current display.
Log Out	Select to log out of the FortiManager Web-based Manager.

The tab bar is located across the top of the window and provides access to all the features of the Fortinet system. The following items are available in the tab bar:

Using the navigation pane

System Settings	Select to configure system settings such as network interfaces, administrators, system time, server settings, including widgets and tabs. From this menu, you can also perform maintenance and firmware operations. For more details on using this menu, see “System Settings” on page 48.
Administrator Domain	Select to add and manage administrator domains.
Device Manager	Select to add and manage devices, view the device information and status, create and manage device groups and manage firewall global policy objects. From this menu, you can also configure the web portal configurations, users and groups. For more details on using this menu, see “Device Management” on page 135.
Policy & Objects	For more details on using this menu, see “Policies and Objects” on page 165.
VPN Console	Select to add and manage VPN consoles. For more details on using this menu, see “VPN Console” on page 177.

Real-Time Monitor	Select to watch your managed devices for trends, outages, or events that require attention. From this menu you can also monitor any FortiGate, FortiSwitch, FortiCarrier or FortiMail device or device group to view system resources and information.
FortiClient Manager	Select to manage FortiClient.

The Web-based Manager navigation pane is located down the left sidebar and provides access to different features and options based on your currently selected tab. For more information on the available options, see the chapter corresponding to your selected tab.

Configuring Web-based Manager settings

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

This section includes the following topics:

- Changing the Web-based Manager language
- Changing administrative access to your FortiManager system
- Changing the Web-based Manager idle timeout

Changing the Web-based Manager language

The Web-based Manager supports multiple languages, but by default appears in English on first use. You can change the Web-based Manager to display language in English, Simplified Chinese, Traditional Chinese, or Japanese. For best results, you should select the language that the management computer operating system uses. You can also set the FortiManager Web-based Manager to automatically detect the system language and by default show the screens in the proper language, if available.

To change the Web-based Manager language:

1. Go to *System Settings* > *Admin* > *Admin Settings*.
2. For *Web Administration*, select the Web-based Manager display language or select *Auto Detect* to use the same language as configured for your web browser.
3. Select *OK*.

FortiManager v4.0 MR3 Patch Release 8 is localized for the following languages:

Language	Web-based Manager	Documentation
English	Yes	Yes
Korean	Yes	-
Chinese (Simplified)	Yes	-
Chinese (Traditional)	Yes	-
Japanese	Yes	-

Changing administrative access to your FortiManager system

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.

You can change administrative access by:

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

To change administrative access to your FortiManager system:

1. Go to *System Settings* > *General* > *Network* and select *All Interfaces*.
2. Select an interface for which to change administrative access.
3. Select one or more *Administrative Access* types for the interface.
4. Select *OK*.

Changing the Web-based Manager idle timeout

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

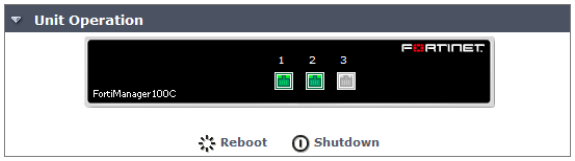
To change the Web-based Manager idle timeout:

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

Reboot and shutdown of the FortiManager unit

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

Figure 5: Unit operation actions in the Web-based Manager



To reboot the FortiManager unit:

1. From the Web-based Manager, go to *System Settings* > *General* > *Dashboard*.
2. In the unit operation widget, select *Reboot* or from the CLI console widget enter the following command:

```
execute reboot
```

To shutdown the FortiManager unit:

1. From the Web-based Manager, go to *System Settings* > *General* > *Dashboard*.
2. In the unit operation widget, select *Shutdown* or from the CLI console widget enter the following command:

```
execute shutdown
```

Administrative Domains

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

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

ADOMs are not enabled by default, and enabling and configuring the domains can only be performed by the `admin` administrator. For more information, see "Enabling and disabling the ADOM feature" on page 39.

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

This section includes the following topics:

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

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 v4.0 MR2 into one ADOM, and all v4.0 MR3 into another.
- Geographic regions; group all devices for a specific geographic region into an ADOM, and devices for a separate region into another ADOM.
- Admin users; group devices into separate ADOMs based for specific administrators responsible for the group of devices.
- Customers; group all devices for one customer into an ADOM, and devices for another customer into another ADOM.
- Device type; create a separate ADOM for each device type, i.e. FortiGate, FortiCarrier, FortiMail, FortiSwitch, and FortiClient 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 it.

To enable the ADOM feature:

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

Figure 6: Enabling ADOMs

System Information	
Host Name	FMG400A [Change]
Serial Number	FMG40A3906500523
HA Status	Standalone
System Time	Fri Feb 22 16:21:57 PST 2013 [Change]
Firmware Version	v4.0-build0700 130220 (MR3 Patch 7) [Update]
System Configuration	Last Backup:Mon Feb 18 14:30:24 2013 [Backup] [Restore] [System Checkpoint]
Current Administrators	admin [Change Password] /10 in Total [Detail]
Up Time	2 days 1 hour 33 minutes 10 seconds
Administrative Domain	Enabled
FortiConsole Software	[Update]

To disable the ADOM feature:

1. Remove the managed devices from all ADOMs.
   - Switch to the ADOM by selecting the *Administrator Domain* tab from the menu bar. For more information see "Switching between ADOMs" on page 40.
   - Select the check boxes for each device and select *Delete*.
2. Delete all non-root ADOMs
   - Select the check box beside the ADOMs and select *Delete*.

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

About ADOM modes

When the ADOMs feature is enabled and you log in as the `admin` user, an *Administrator Domain* tab appears at the top navigation pane. You can choose one of two administrative modes:

- *Global*: This mode enables you to configure, set up and manage ADOMs. For more information about working in global mode, see "Managing ADOMs" on page 41.
- *ADOM (name):* If any ADOMs have been configured, the individual ADOM names will appear in the drop down list. Selecting an ADOM name will display the ADOM properties. From here you can view the specific devices belonging to the selected ADOM. For more information about working in ADOM mode, see "Managing ADOMs" on page 41.

When the ADOMs feature is enabled, the *Administrator Domain* tab and only lists all of the ADOMS when you log into the FortiManager unit as the `admin` user. All other administrators can select only from the ADOMs which they have been assigned.

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. When you log into the FortiManager system as the `admin` administrator, by default you log in to the *Global* mode.

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

To access a specific ADOM, from the ADOM mode drop-down list at the bottom of the navigation tree, select the ADOM you want to enter.

Once switched over to the new ADOM, the FortiManager system presents you with the *Device Manager* view for that domain. You will also have additional menu selections in the navigation pane for Policy, Objects, VPN Console, and Real-Time Monitor.

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 Web-based Manager or CLI directly.

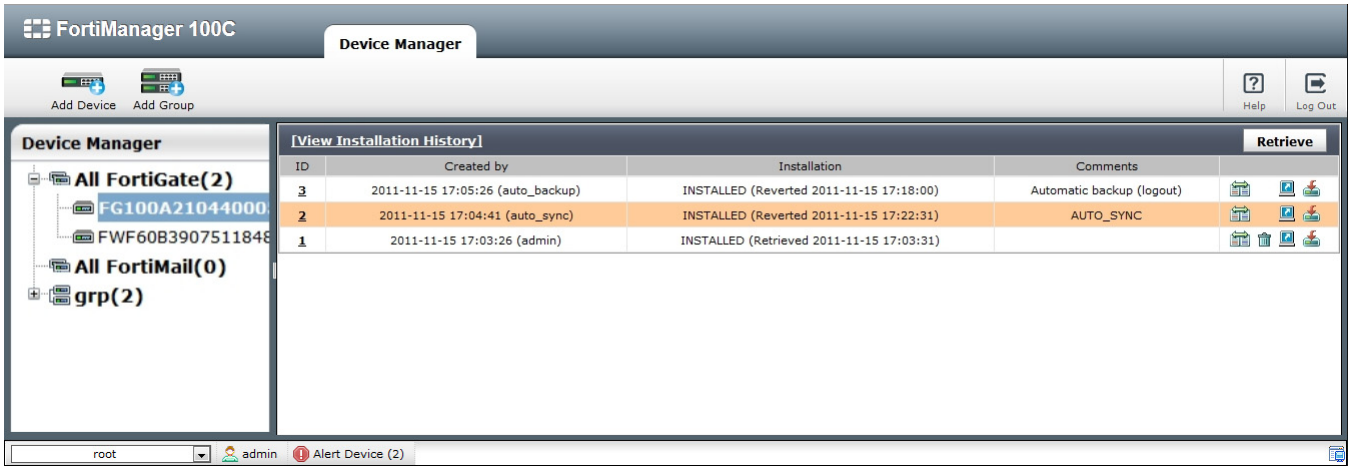
Revisions are sent to the FortiManager when specific conditions are met:

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

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

Figure 7 shows the revision of a device in a backup mode ADOM.

Figure 7: Backup mode ADOM device revision history



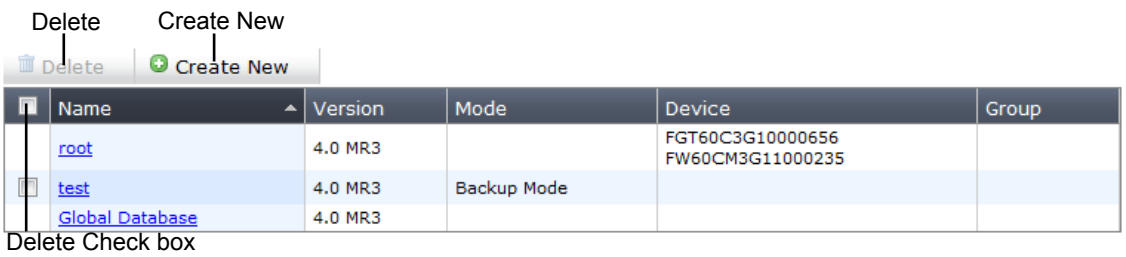
Managing ADOMs

When the ADOMs feature is enabled, the *Administrative Domain* menu appears on the bottom left navigation pane. To configure and manage ADOMs, select the *Global* mode from the drop-down list at the bottom of the navigation pane. In this mode you can manage the ADOMs and device assignments.

The Administrator Domain tab appears only when you log in as the `admin` user.

Go to *Administrative Domain* > *All ADOMs*. The ADOM table appears; see Figure 8. The following information is available:

Figure 8: ADOM table



The following options are available

Delete check box	Select the check box when you want to remove one or more ADOMs. Select Delete (located above the table) to remove the domain or domains. **Note:** Before you can delete an ADOM, you must first remove all devices from that domain. See “Removing devices from a domain.”
Create New	Select to create a new ADOM. See “Adding an ADOM” on page 42.
Name	The name of the ADOM. Select the name to enter that ADOM. The new domain information will be displayed in the Main Menu Bar.
Version	The global database version and release of the objects to configure for the devices.
Mode	The ADOM mode, such as *Backup Mode* (see “Backup mode ADOMs” on page 40).
Device	A list of devices in the ADOM.
Group	A list of groups of devices in the ADOM.

Concurrent ADOM access

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

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

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

To enable ADOM locking and disable concurrent ADOM access:

```
config fmsystem global
  set workspace enable
end
```

To disable ADOM locking and enable concurrent ADOM access:

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

Adding an ADOM

To add an ADOM, you must be logged in as the `admin` administrator. You must also first enable administrative domains in the Web-based Manager; see “To enable the ADOM feature:” on page 39.

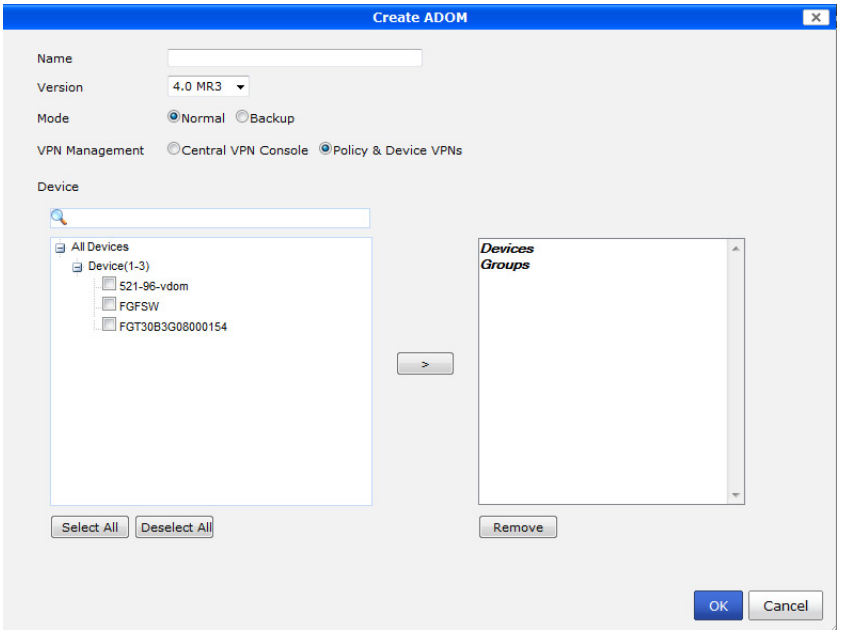
To create an ADOM:

1. Log into the FortiManager Web-based Manager using an administrator account. The Administrator Domain tab is the default window on login.
2. To create a new ADOM you can either select Create New from the top menu pane or right click the body pane and select New from the right-click menu.
3. Select Create New from the top menu pane to create a new ADOM. A Create ADOM window will pop-up which will allow you to configure the new ADOM. Enter the following information:
   - Name: Enter a name that will allow you to distinguish this ADOM from your other ADOMs.
   - Version: Select the version of FortiGate devices in the ADOM. FortiManager v4.0 MR3 can manage FortiOS v4.0 MR2 and MR3.
   - Mode: Select *Normal* mode if you want to manage and configure the connected FortiGate devices from the FortiManager Web-based Manager. Select *Backup* mode if you want to backup the FortiGate configurations to the FortiManager, but configure each FortiGate locally.
   - VPN Management: Select *Central VPN Console* or Select *Policy & Device VPNs*.
   - Devices: Select which devices to add to the ADOM.
4. Select *OK* to create the ADOM.

FortiManager Cookbook video link

http://www.youtube.com/watch?v=1OMlRjx9eYE&list=PL29F8DE57AA4CA091&index=5&feature=plpp_video

Figure 9: Add an ADOM



Configure the following settings:

Name	Enter a name for the ADOM.
Version	Select the firmware release for the ADOM from the drop-down list.
Mode	Normal or Backup Mode

VPN Management	Central VPN Console or Policy & Device VPNs
Device	Select members from the *Available member* list and transfer them to the *Selected member* list.

Deleting an ADOM

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

To delete an ADOM:

1. In the navigation pane, select *Global* from the ADOM drop-down menu.
2. *Administrative Domain* > *All ADOMs*. The ADOM table appears; see Figure 8.
3. Do one of the following:
   - Select the check box next to the ADOM you want to delete and from the menu above the table select *Delete*.
   - Right-click on the ADOM you want to delete and select *delete* from the pop-up menu.
4. In the confirmation dialog box, select *OK*.

Assigning devices to an ADOM

The `admin` administrator selects the devices to be included in an ADOM. You cannot assign the same device to two different domain modes. For a description of the differences, see "About ADOM modes" on page 40.

To assign devices to an ADOM:

1. In the navigation pane, select *Global* from the ADOM drop-down menu.
2. Select *Administrator Domain* in the navigation pane.
3. Double-click, or right-click and select edit, on the domain you want to configure. A dialog box appears.
4. From the *Available member* list, select which devices you want to associate with the ADOM and select the *Right arrow* to move them to the *Selected member* list.

   If the administrative device mode is *Advanced*, you can add separate FortiGate VDOMs to the ADOM as well as FortiGate units. For more information see "ADOM device modes" on page 44.
5. When done, select *OK*. The selected devices appear in the Device column for the ADOM in the ADOM table.

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

ADOM device modes

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

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

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

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

Normal mode is the default. To change from advanced back to normal, you must ensure no FortiGate VDOMs are assigned to an 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 44.

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.

Viewing ADOM assignments

The *Administrative Domain* > *Assignment* page lists the configured global policy packages and the ADOMS to which the packages have been assigned.

The following information is available for each global policy package:

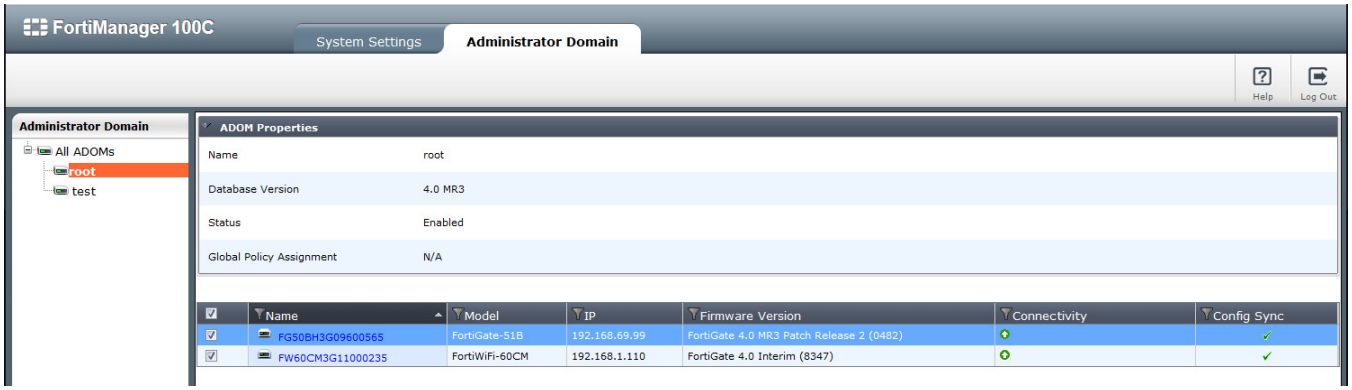
No Global Policy	Lists ADOMs for which global policy packages are not used.
Global Policy Package Name	Lists all the ADOMs to which the named global policy package has been assigned.
ADOM Name	The name of the ADOM
Version	The ADOM FortiManager OS version
Devices	The list of devices assigned to the ADOM. A tooltip displays the full list of devices when you hover your mouse over the field.

Assignment Status	An icon indicating the global policy package assignment status. A green checkmark indicates that the ADOM is in compliance with the assigned global policy package. A white x on a red background indicates that the ADOM is out of synch with the assigned global policy package.
Last Assigned	The date and time that the global policy package was last assigned to the selected ADOM.
Last Assigned By	The name of the administrator who last assigned the global policy package to the selected ADOM.

Viewing ADOM properties

You can view the properties and device status for any configured ADOM by viewing the ADOM dashboard for that domain. To access the ADOM dashboard for a domain, go to *Administrative Domain* > *All ADOMs* menu and from the navigation tree, select the ADOM that you want to view. The ADOM dashboard for that domain appears in the content pane. The following widgets are available:

Figure 10:ADOM dashboard example



The following information and options are available:

ADOM Properties **widget**	Select this widget to view or modify ADOM properties.
Name	The name of the ADOM Select *Go* to access the domain in ADOM mode.
Database Version	The FortiManager database version in which the ADOM was created.
Status	The ADOM status: *enabled* or *disabled*.
Migration Mode	Indicates whether migration mode from an earlier FortiManager global database version is *enabled* or *disabled*.
Global Policy Assignment	Lists the global policy packages assigned to this ADOM.
Administrators	Lists the administrators assigned to this ADOM.
Device list	Lists the devices assigned to this ADOM and their status. You can filter the list by selecting any filter icon in the column headings.

Name	Device name
Model	Device model number
IP	Device IP address
Firmware Version	Current firmware version installed on the device
Connectivity	Connection status
Contact	Contact information.

System Settings

The *System Settings* tab enables you to manage and configure the basic system options for the FortiManager unit. This includes the basic network settings to connect the device to the corporate network, the configuration of administrators and their access privileges, managing and updating firmware for the device and configuring logging and access to the FortiGuard update service for updates.

If the administrator account you logged on with does not have system tab privileges, you will not be able to edit or delete settings, or apply any changes. Instead you are limited to browsing. To modify these settings, see “Configuring administrator profiles” on page 85.

The *System Settings* menu provides access to the following submenus:

General	Select this submenu to configure and monitor the main system information. For more information, see “Configuring general settings” on page 60.
Admin	Select this menu to configure administrator user accounts, as well as configure global administrative settings for the FortiManager unit. For more information, see “Managing administrators” on page 78.
FortiGuard Update Service	Select to view the version and status of antivirus, attack and antispam versions, and enables you to configure override servers and push update settings. For more information, see “Managing FortiGuard Services” on page 94.
Advanced	Select to configure mail server settings, remote output, SNMP, metafield data and other advanced settings. For more information, see “Configuring advanced settings” on page 98.

This section describes the following topics:

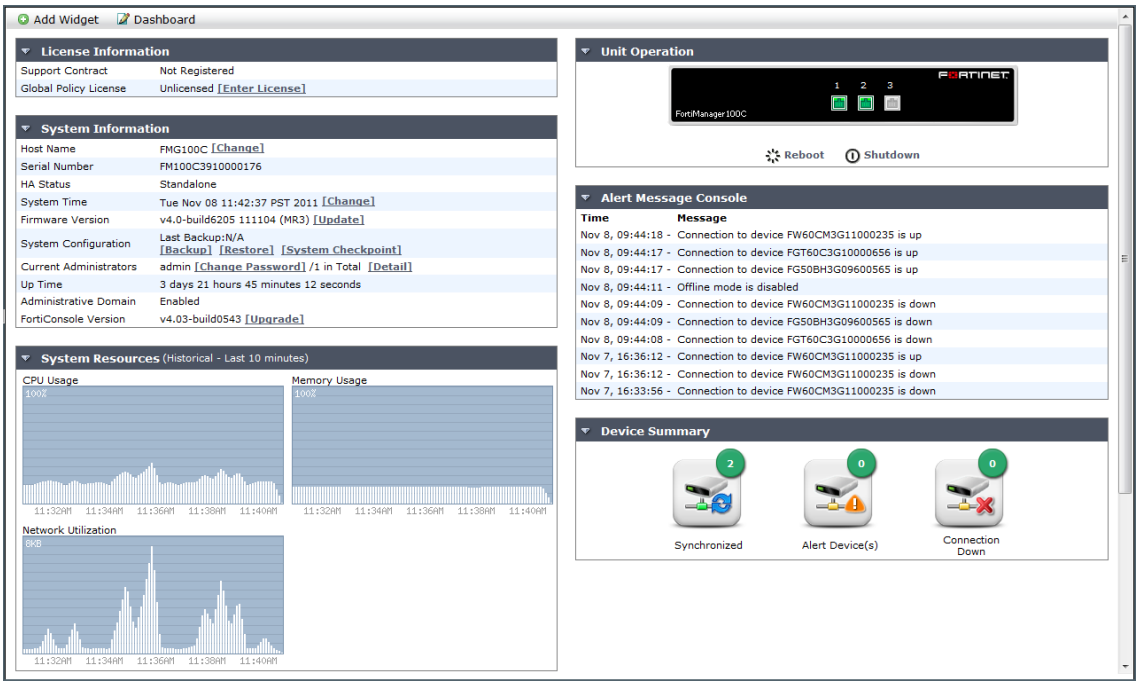
- Viewing the system status
- Configuring general settings
- Managing administrators
- Managing FortiGuard Services
- Viewing local event logs
- Configuring advanced settings

Viewing the system status

When you log in to the FortiManager Web-based Manager, it automatically opens at the *System Settings* > *General* > *Dashboard* page; see Figure 11.

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

Figure 11: FortiManager system dashboard



The following widgets are available:

System Information	Displays basic information about the FortiManager system, such as up time and firmware version. For more information, see "Configuring general settings" on page 60. From this widget you can also manually update the FortiManager firmware to a different release. For more information, see "Firmware and Revision Control" on page 264.
System Resources	Displays the real-time and historical usage status of the CPU, memory and hard disk. For more information, see "Viewing system resource information" on page 53.
License Information	Displays the devices being managed by the FortiManager unit and the maximum numbers of devices allowed. For more information, see "Viewing license information" on page 55.
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 "Viewing unit operation" on page 55.

Alert Message Console	Displays log-based alert messages for both the Fortinet unit itself and connected devices. For more information, see “Viewing alert messages” on page 58.
RAID Monitor	Displays information about the status of RAID disks as well as what RAID level has been selected. It also displays how much disk space is currently consumed. For more information, see “Viewing RAID status” on page 56.
CLI Console	Opens a terminal window that enables you to configure the FortiManager unit using CLI commands directly from the Web-based Manager. This widget is hidden by default. For more information, see “Using the CLI console widget” on page 59.
Device Summary	For more information, see “Viewing the device summary” on page 55.

Customizing the dashboard

The FortiManager system dashboard is customizable. You can select which widgets to display, where they are located on the page, and whether they are minimized or maximized. You can also create additional dashboards.

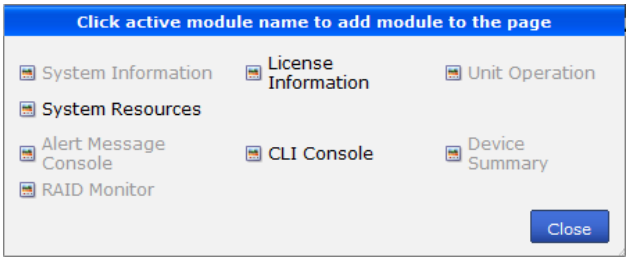
To move a widget

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

To add a widget

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

Figure 12: Adding a widget



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

To see the available options for a widget

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

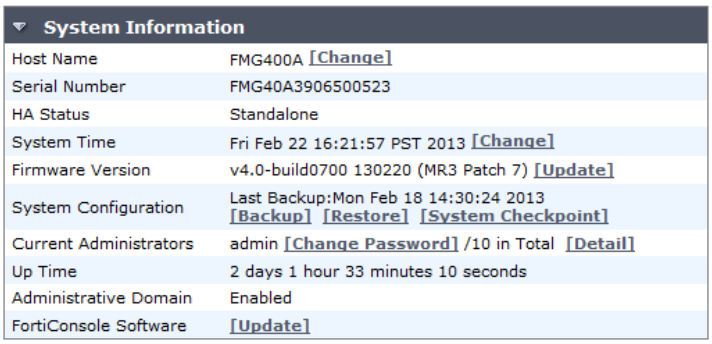
Figure 13:A minimized widget

Show/Hide arrow	Display or minimize the widget.
Widget Title	The name of the widget.
More Alerts	Show the Alert Messages dialog box. This option appears only on the Alert Message Console widget.
Edit	Select to change settings for the widget. This option appears only on certain widgets.
Detach	Detach the CLI Console widget from the dashboard and open it in a separate window. See “Using the CLI console for managed devices” on page 163. This option appears only on the CLI Console widget.
RAID Settings	Show the RAID Settings dialog box, which displays the current RAID settings and allows for configuration of the RAID level if available. This option appears only on the RAID Monitor widget.
Refresh	Select to update the displayed information.
Close	Select to remove the widget from the dashboard. You will be prompted to confirm the action. To add the widget, select *Widget* in the toolbar and then select the name of the widget you want to show.

Viewing system information

The system dashboard includes a *System Information* widget, shown in Figure 14, which displays the current status of the FortiManager unit and enables you to configure basic system settings.

Figure 14: System information widget



The following information is available on this widget:

Host Name	The identifying name assigned to this FortiManager unit. For more information, see "Changing the host name" on page 61.
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 356.
System Time	The current time on the FortiManager internal clock. To change the time, select *Change*. For more information, see "Configuring the system time" on page 61.
Firmware Version	The version number and build number of the firmware installed on the FortiManager unit. To update the firmware, you must download the latest version from the Customer Service & Support web site at https://support.fortinet.com. Select *Update* and select the firmware image to load from the local hard disk or network volume. For more information, see "Updating the system firmware" on page 63.
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 configuration" on page 65. • Select *Restore* to restore the configuration from a backup file; see "Restoring the configuration" on page 65. • Select *System Checkpoint* to revert the system to a prior saved configuration; see "Creating a system checkpoint" on page 66.

Current Administrators	The number of administrators that are currently logged in. The following actions are available: • Select *Change Password* to change your own password. • Select *Details* to view the session details for all currently logged in administrators.
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.

FortiConsole Software	Displays the current version of FortiConsole.
	Enter the following CLI command to enable FortiConsole options:
	`config fmsystem global`
	`  set show-forticonsole enable`
	`end`

Viewing system resource information

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

Figure 15: System resources widget (Real time display)

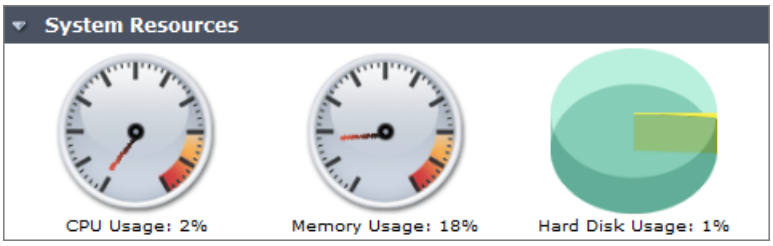
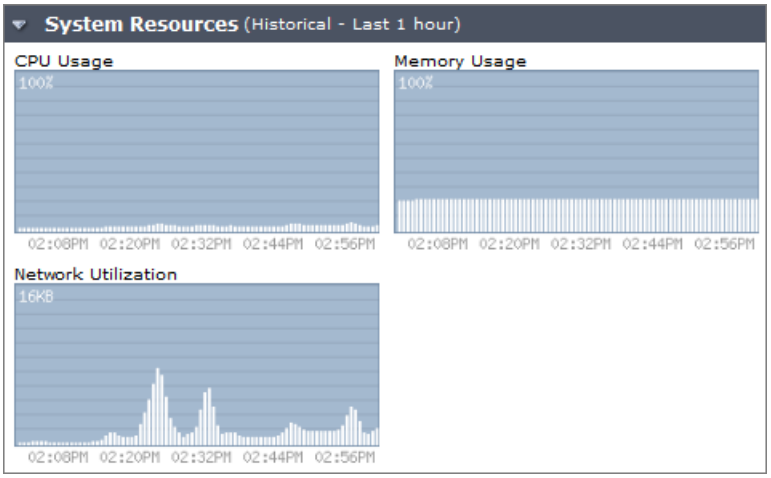


Figure 16: System resource widget (Historical display)



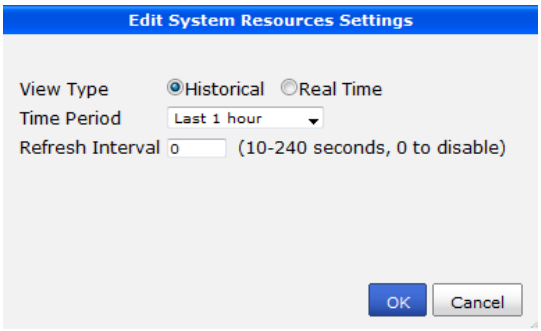
The following information is available on this widget:

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

To change system resource widget display settings:

1. Go to *System Settings* > *General* > *Dashboard*.
2. In the system resources widget, hover the mouse over the title bar and select the *Edit* icon. The edit system resources settings dialog box appears.

   Figure 17: Edit system resources settings window

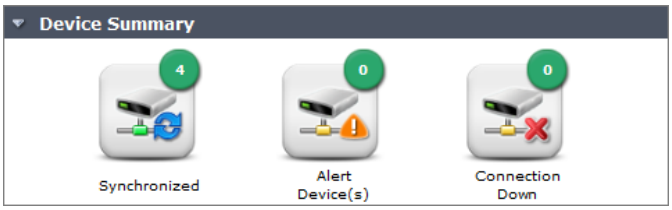


3. You can configure the following settings:
   - To view only the most current information about system resources, from *View Type*, select *Real Time*. This is the default.
   - To view historical information about system resources, from *View Type*, select *History*. To change the time range, from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

Viewing the device summary

The *Device Summary* widget on the dashboard displays the number of devices that are synchronized, disconnected, or are in alert status.

Figure 18: Device Summary widget



Synchronized	The number of devices that are synchronized with the FortiManager unit.
Alert Device (s)	The number of devices with alert messages. Select the icon to view the list of alert devices.
Connection Down	The number of devices with which the FortiManager unit has lost connection. Select the icon to view the list of disconnected devices.

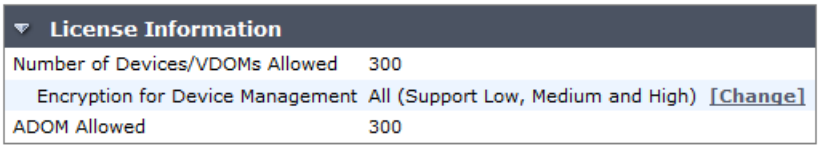
Viewing license information

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

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

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

Figure 19:VM license information widget



Viewing unit operation

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

Figure 20: Unit operation widget

The following information is displayed on this widget:

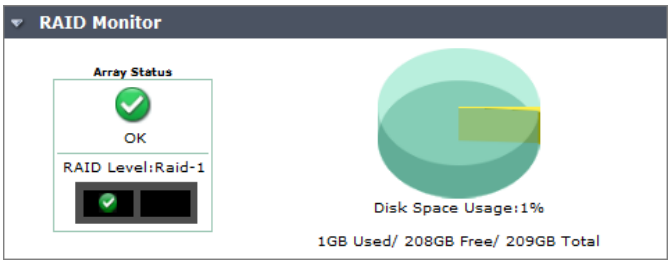
Port numbers (vary depending on model)	The image below the port name indicates its status by its color. Green indicates the port is connected. Grey indicates there is no connection. For more information about a port's configuration and throughput, position your mouse over the icon for that port. You will see the full name of the interface, the IP address and network mask, 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.

Viewing RAID status

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

The RAID Monitor layout is similar to the look of the front panel. The Drive Status Indicator allows you to view each disk's name, a pie chart of the disk's usage, and the amount of space in GB each has.

Figure 21:RAID monitor displaying a RAID array without any failures



The drive status indicator will also show when a disk has failed. This is displayed by both a warning symbol and text. The text appears when you hover your mouse over the warning symbol. When a disk has failed, caution triangle icon appears in the drive status indicator.

The following information is available:

Array Status	Icons and text indicating the RAID level and one of the following RAID disk statuses: • *green checkmark (OK)*: Indicates that the RAID disk has no problems • *warning symbol (Warning)*: Indicates that there is a problem with the RAID disk, such as a failure, and needs replacing. The RAID disk is also in reduced reliability mode when this status is indicated in the widget. • *wrench symbol (Rebuilding)*: Indicates that a drive has been replaced and the RAID array is being rebuilt; it is also in reduced reliability mode. • *exclamation mark (Failure)*: Indicates that one or more drives have failed, the RAID array is corrupted, and the drive must be re-initialized. This is displayed by both a warning symbol and text. The text appears when you hover your mouse over the warning symbol; the text also indicates the amount of space in GB.
Rebuild Status	A percentage bar indicating the progress of the rebuilding of a RAID array. The bar displays only when a RAID array is being rebuilt.
Estimated rebuild time [start and end time]	The time remaining to rebuild the RAID array, and the date and time the rebuild is expected to end. This time period displays only when an array is being rebuilt. This time period will not display in hardware RAID, such as FMG-2000, FMG-2000A, FMG-2000B, FMG-4000, FMG-4000A, FMG-4000B.
Rebuild Warning	Text reminding you the system has no redundancy protection until the rebuilding process is complete. This text displays only when an array is being rebuilt.
Disk space usage	The amount of disk used, displayed as a percentage and a percentage pie chart, and listing the number of GB used, free, and in total. Note that the FortiManager unit reserves some disk space for compression files, upload files, and temporary reports files. The total reserved space is: • 25% of total disk space if total < 500G, with MAX at 100G • 20% of total disk space if 500G< total <1000G, with MAX at 150G • 15% of total disk space if 1000G < total < 3000G, with MAX at 300G • 10% of total disk space if total > 3000G This is therefore to be deducted from the total capacity.

Fortinet units allocate most of their total disk space for both the Fortinet unit's own logs as well as logs and quarantined files from connecting devices. Disk space quota is assigned to each device and the Fortinet unit itself. If the quota is consumed, the Fortinet unit will either overwrite the oldest files saved or stop collecting new logs, depending on your preference.

Remaining disk space is reserved for devices, FortiAnalyzer reports, and any temporary files, such as configuration backups and log files that are currently queued for upload to a server. The size of the reserved space varies by the total RAID/hard disk capacity. For more information, see "Disk space usage" on page 57.

For more information about RAID, see "Configuring RAID" on page 67.

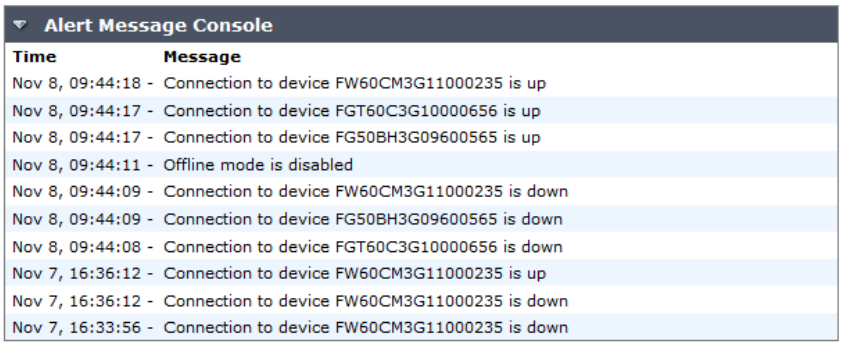
Viewing alert messages

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

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

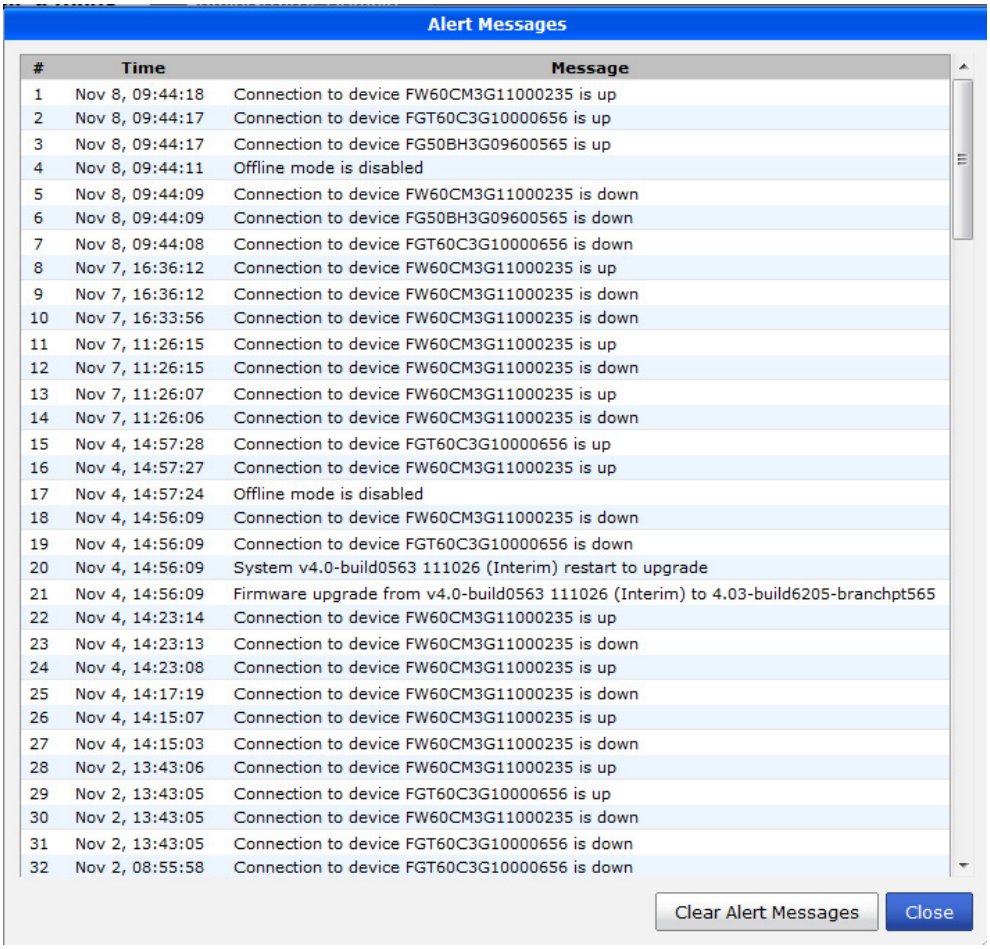
Alert messages can also be delivered by email, syslog or SNMP.

Figure 22: Alert message console widget



The widget displays only the most current alerts. For a complete list of unacknowledged alert messages (see Figure 23), select the *More Alerts* icon in the widget's title bar. A popup window appears. To clear the list, select *Clear Alert Messages*.

Figure 23: List of all alert messages



Using the CLI console widget

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

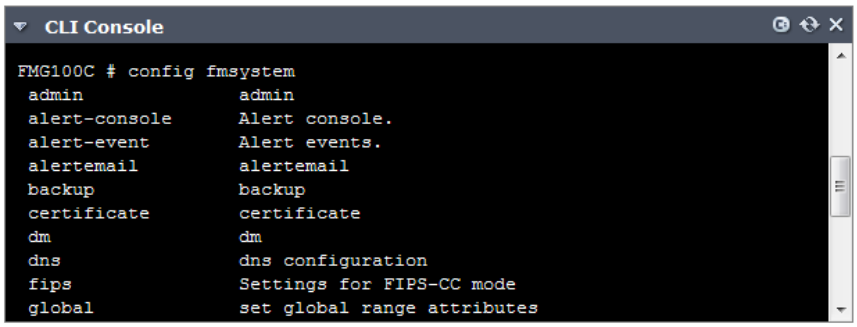
The *CLI Console* widget requires that your web browser support JavaScript.

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

The prompt, by default the model number such as `Fortinet-800B #`, contains the host name of the Fortinet unit. To change the host name, see “Changing the host name” on page 61.

For information on available commands, see the *FortiManager v4.0 MR3 Patch Release 7 CLI Reference*.

Figure 24:CLI console widget



Configuring general settings

The *System Settings* > *General* menu provides options that enable you configure and monitor the system information of the FortiManager unit. The following options are available:

Dashboard	Select to monitor the system status and performing general configuration tasks such as setting time, RAID configuration, system backup and restore operations and firmware updates or the FortiManager unit. For more information, see "Viewing the system status" on page 49.
Network	Select to configure FortiManager network interfaces, routing, and DNS settings. For more information, see "Configuring network settings" on page 70.
Certificates	Select to add local certificates and CA certificates. For more information, see "Managing certificates" on page 74.
HA	Select to configure high-availability load balancing or redundancy between multiple FortiManager units to ensure no single point of failure for network management. For more information, see "Configuring High Availability" on page 76.
Local Log	View current logs.
Diagnostic Tools	Select to run available diagnostic tools, including *Ping* and *Traceroute*.

This section includes the following topics:

- Changing the host name
- Configuring the system time
- Updating the system firmware
- Backing up and restoring the system
- Configuring RAID
- Configuring network settings
- Managing certificates
- Configuring High Availability

Changing the host name

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

- It appears in the *System Information* widget on the *Dashboard*. For more information about the *System Information* widget, see "Viewing system information" on page 52.
- It is used in the command prompt of the CLI.
- It is used as the SNMP system name. For information about SNMP, see "Configuring SNMP" on page 98.

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

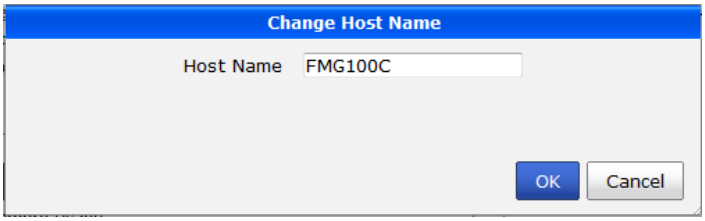
For example, if the host name is Fortinet1234567890, the CLI prompt would be `Fortinet123456~#`.

To change the host name:

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

   The change host name dialog box appears.

   Figure 25: Edit host name dialog box



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

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

Configuring the system time

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

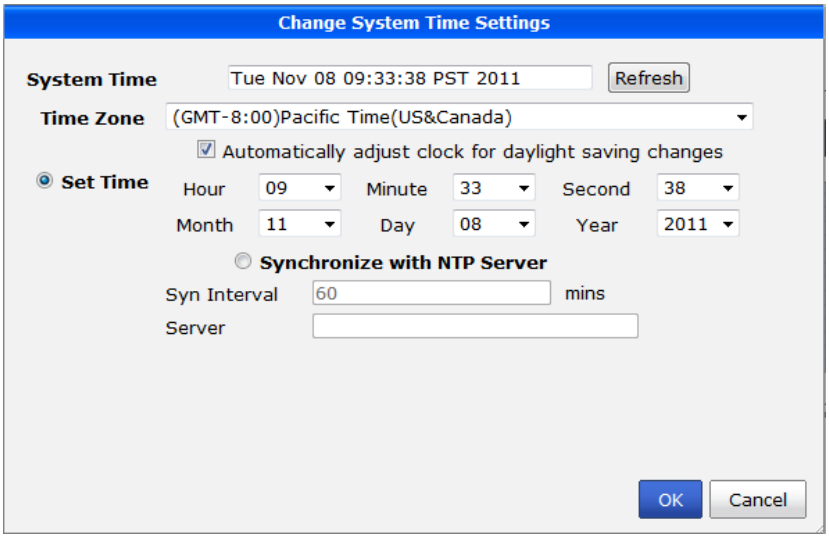
For many features to work, including scheduling, logging, and SSL-dependent features, the Fortinet system time must be accurate.

To configure the date and time:

1. Go to *System Settings* > *General* > *Dashboard*.
2. In the *System Information* widget, in the *System Time* row, select *Change*.

   The change system time settings dialog box appears.

Figure 26: Time settings dialog box



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

System Time	The date and time according to the Fortinet unit's clock at the time that this tab was loaded, or when you last selected the *Refresh* button.
Refresh	Select to update the *System Time* field with the current time according to the Fortinet unit's clock.
Time Zone	Select the time zone in which the Fortinet unit is located and whether or not the system automatically adjusts for daylight savings time.
Set Time	Select this option to manually set the date and time of the Fortinet unit's clock, then select the *Hour*, *Minute*, *Second*, *Year*, *Month* and *Day* fields before you select *OK*.
Synchronize with NTP Server	Select this option to automatically synchronize the date and time of the Fortinet unit's clock with an NTP server, then configure the <GUIElement>Server and <GUIElement>Sync Interval fields before you select *OK*.
Sync Interval	Enter how often in minutes the Fortinet unit should synchronize its time with the NTP server. For example, entering 1440 causes the Fortinet unit to synchronize its time once a day.
Server	Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, go to http://www.ntp.org.

4. Select *OK* to apply your changes.

Updating the system firmware

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

Back up the configuration and database before changing the firmware of your Fortinet unit. Changing the firmware to an older or incompatible version may reset the configuration and database to the default values for that firmware version, resulting in data loss. For information on backing up the configuration, see “Backing up and restoring the system” on page 64.

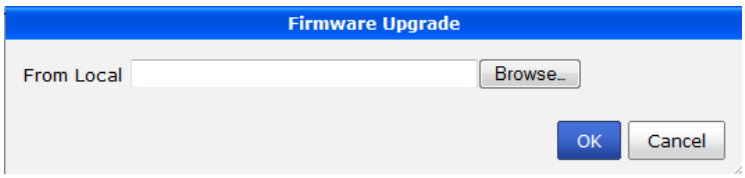
Before you can download firmware updates for your Fortinet unit, you must first register your Fortinet unit with Customer Service & Support. For details, go to https://support.fortinet.com/ or contact Customer Service & Support.

To manually change the Fortinet firmware:

1. Download the firmware (the `.out` file) from the Customer Service & Support web site, https://support.fortinet.com/.
2. Go to *System Settings* > *General* > *Dashboard*.
3. In the *System Information* widget, in the *Firmware Version* row, select *Update*.

   The firmware upgrade dialog box opens.

   Figure 27: Firmware upgrade dialog box

4. Select *From Local*, and select *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support web site and select *Open*.
5. Select *OK* to upload the file.

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

   “`Manual upload release complete. It will take a few minutes to unpack the uploaded release. Please wait.`”
6. Wait until the unpacking process completes, then refresh the page. The firmware package file name will appear in the *Releases Available For Upgrade* section after you refresh the page.
7. Select the firmware package, then select the icon in the *Upgrade Firmware* column and select *OK* in the dialog box that appears. The Fortinet unit installs the firmware and restarts.

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

8. Update the vulnerability management engine and definitions. For details, see “FortiGuard Services” on page 242.

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 Services” on page 242.

To change the FortiManager system firmware through FDN:

1. The FortiManager system can automatically download firmware updates from FDN, if you have a valid support license. To access these updates, go to *System* > *Dashboard* > *Status*.
2. In the *System Information* widget, in the *Firmware Version* row, select *Update*. The Firmware Upgrade dialog box appears; see Figure 27.

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

Upgrading firmware through FDN needs proper setup.

FortiManager v4.0 MR3 does not provide a full downgrade path. For those users who want to downgrade to an older FortiManager firmware release, downgrade the system firmware via a TFTP server with the firmware burning procedure embedded within the FortiManager system boot-up menu. A full format of the system hard drives and system reset are required after the firmware downgrading process.

All configuration will be lost after downgrading the device, and the system hard drives will be formatted.

For more information on upgrading or downgrading the firmware, see “Firmware and Revision Control” on page 264.

Backing up and restoring the system

Fortinet recommends that you back up and restore 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.

Backing up the configuration

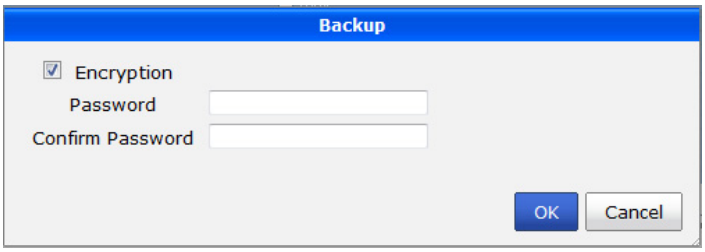
The following procedures enable you to back up your current configuration through the web-based manager. If your FortiManager unit is in HA mode, switch to Standalone mode.

To back up the FortiManager configuration:

1. Go to *System Settings* > *General* > *Dashboard*.
2. In the System Information widget, under *System Configuration*, select the *Backup*.

   The backup dialog box appears.

Figure 28: Backup dialog box



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 encryption check box is selected.)
Confirm Password	Re-enter the password to confirm it.

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

Restoring the configuration

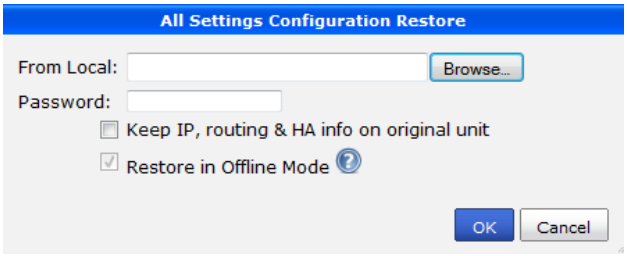
You can use the following procedure to restore your FortiManager configuration from a backup file on your management computer. If your FortiManager unit is in HA mode, switch to Standalone mode.

To restore the FortiManager configuration:

1. Go to *System Settings* > *General* > *Dashboard*.
2. In the system information widget, under *System Configuration*, select *Restore*.

   The all settings configuration restore dialog box appears.

Figure 29: All settings configuration restore dialog box



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

From Local	Select the configuration backup file you want to restore.
Password	Enter the encryption password, if applicable.
Keep IP, routing & HA info on original unit	Select the check box to retain the current IP, routing and HA settings.
Restore in Offline Mode	Informational check box. Hover over help icon for more information.

Scheduling backups

You can schedule backups at a regular interval to ensure that you have a backup of the FortiManager configuration, no matter when changes are made. It also ensures you do not forget to backup the configuration. This feature is only available from the CLI interface, which you can access from the CLI console widget on the system dashboard. Use the command:

```
config fmsystem backup all-settings
```

For details on how to use this command, see the *FortiManager v4.0MR3 Patch Release 7 CLI Reference*.

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 synchronized. Should there be a major failure, you can completely revert to the network to when it was in working order, and not have to be concerned about which device has which versions of the firmware installed and so on. These are, in essence, snapshots of your Fortinet managed network system.

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

A system checkpoint backup includes:

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

To create a checkpoint backup:

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

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

Configuring RAID

RAID (Redundant Array of Independent Disks) helps to divide data storage over multiple disks which provides increased data reliability. FortiManager units that contain multiple hard disks (typically, the FMG-3000B or higher) can configure the RAID array for capacity, performance and availability.

You can view the status of the RAID array from the RAID Monitor widget on the *System Settings* > *General* > *Dashboard* page. The RAID Monitor widget displays the status of each disk in the RAID array, including the disk's RAID level. This widget also displays how much disk space is being used. For more information, see "Viewing RAID status" on page 56.

The *Alert Message Console* widget, located in *System Settings*> *General* > *Dashboard* provides detailed information about RAID array failures. For more information see "Viewing alert messages" on page 58.

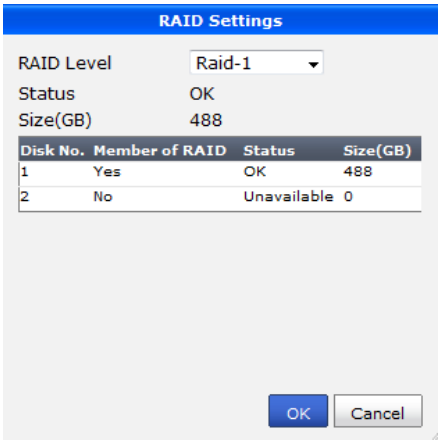
If you need to remove a disk from the FortiManager unit, you can hot swap it. Hot swapping means that you can remove a failed hard disk and replace it with a new one even while the FortiManager unit is still in operation. Hot swapping is a quick and efficient way to replace hard disks. For more information about hot swapping, see "Replacing hard disks" on page 68.

To configure RAID:

1. Go to *System Settings* > *General* > *Dashboard*.
2. From the RAID monitor widget title bar, select *RAID Settings*.

   The RAID Settings dialog box appears.

Figure 30:RAID settings dialog box



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

Supported RAID levels

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

- **RAID 0**

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

- **RAID 1**

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

- **RAID 5**

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

- **RAID 10**

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

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

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

Replacing hard disks

If a hard disk on a FortiManager unit fails, it must be replaced.

The *Disk Monitor* widget indicates a failed disk, including its RAID level, but does not give specific information about when the disk failed. To identify which hard disk failed, read the relevant log message in the *Alert Message Console* widget (see "Alert message console widget" on page 58).

To replace a hard disk:

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.

1. Go to *System* > *General* > *Dashboard*.
2. In the *Unit Operation* widget, click *Shutdown*.
3. Click *OK*.
4. Remove the faulty hard disk and replace it with a new one.
5. Restart the FortiManager unit.

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

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

See also

- Viewing RAID status
- Adding new disks for FMG-2000B and FMG-4000B
- Configuring RAID

Adding new disks for FMG-2000B and FMG-4000B

The FMG-2000B unit is shipped with two hard disks. You can add up to four more disks to increase the storage capacity. The FMG-4000B unit is shipped with six hard disks. You can add up to 18 more disks to increase the 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 FMG-2000B/FMG-4000B 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 configuration” on page 65.

3. Install the disks on the FortiManager unit. You can do so while the FortiManager unit is running.
4. Configure the RAID level. See “Configuring RAID” on page 67.
5. If you have backed up the log data, restore the data. For more information, see “Restoring the configuration” on page 65.

See also

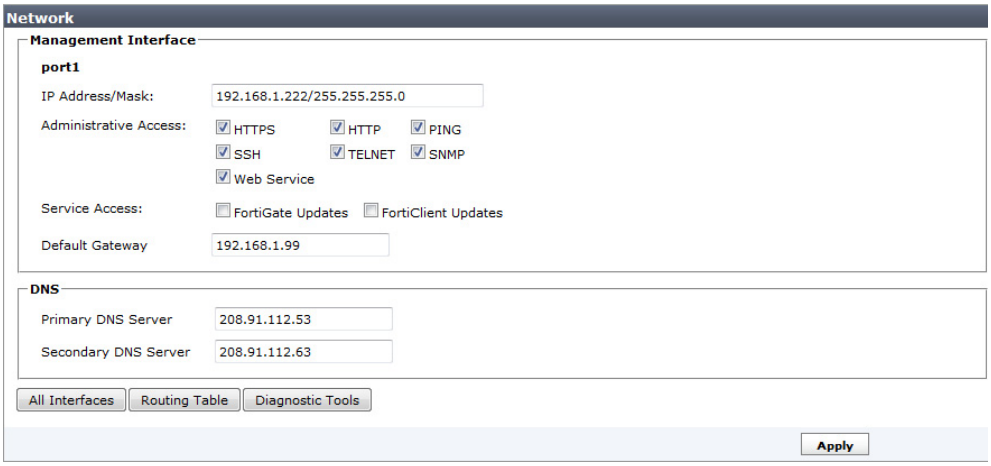
- Viewing RAID status
- Replacing hard disks
- Configuring RAID

Configuring network settings

The FortiManager unit can manage Fortinet devices connected to any of its interfaces. The only exception being if the FortiManager unit is operating as part of an HA cluster, in which case, the interface used for HA operation is not available for other uses. The DNS servers must be on the networks to which the FortiManager unit connects, and should be two different addresses.

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

Figure 31: Network screen



The following information is available:

Management interface port information	
IP Address/Mask	The IP address and network mask associated with this interface.
Administrative Access	Select the allowed 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 FortiClient updates. By default all service access is enabled on port1, and disabled on port2.
Default Gateway	The default gateway associated with this interface

DNS information	
Primary DNS Server	Enter the primary DNS server IP address.
Secondary DNS Server	Enter the secondary DNS server IP address.
All Interfaces	Click to open the network interface list. See “Viewing the network interface list” on page 71.
Routing Table	Click to open the routing table. See “Configuring static routes” on page 72.
Diagnostic Tools	Click to open the diagnostic tools console.

Viewing the network interface list

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

Figure 32: Network interface list

Name	IP/Netmask	Description	Administrative Access	Service Access	Enable
port1	10.100.22.41 / 255.255.255.0		HTTPS, HTTP, PING, SSH, TELNET, SNMP, Web Service	FortiGate Updates, FortiClient Updates	✓
port2	192.168.15.41 / 255.255.255.0		HTTPS, HTTP, PING, SSH, TELNET, SNMP, Web Service	FortiGate Updates, FortiClient Updates	✓
port3	0.0.0.0 / 0.0.0.0				✓
port4	0.0.0.0 / 0.0.0.0				✓

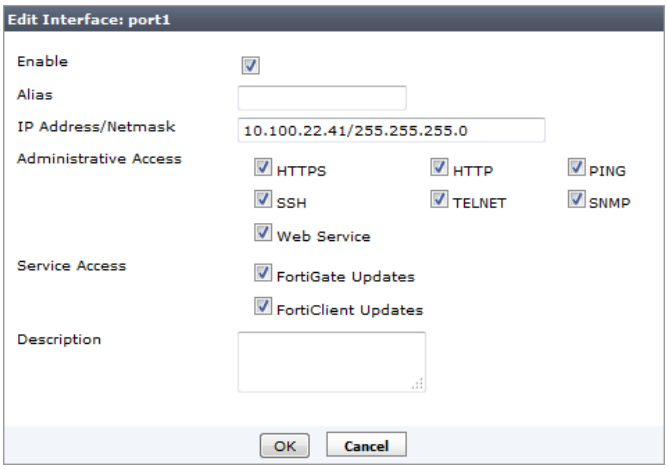
The following information is available:

Name	The names of the physical interfaces on your FortiManager unit. The name, including number, of a physical interface depends on the model. Unlike FortiGate, you cannot set alias names for the interfaces. For more information, on configuring the interface, see “Configuring network interfaces” on page 72. If HA operation is enabled, the HA interface has */HA* appended to its name.
IP / Netmask	The IP address and network mask associated with this interface.
Description	
Administrative Access	The list of allowed administrative service protocols on this interface. These include HTTP, HTTPS, PING, SSH, and Telnet.
Service Access	The list of Fortinet services that are allowed access on this interface. These include FortiGate updates, FortiClient updates, Web Filtering, and email filtering. By default all service access is enabled on port1, and disabled on port2.
Enable	Displays if the interface is enabled or disabled. If the port is enabled, a green circle with a check mark appears in the column. If the interface is not enabled, a gray circle with an “X” appears in the column.

Configuring network interfaces

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

Figure 33: Configure network interfaces



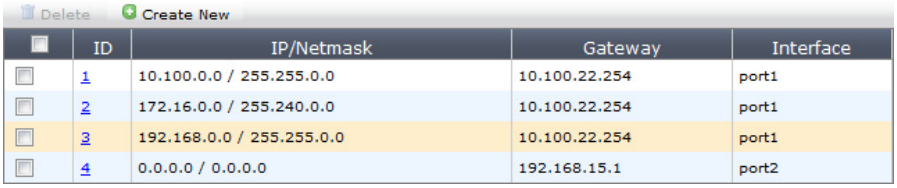
Configure the following settings:

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

Configuring static routes

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

Figure 34: Routing table



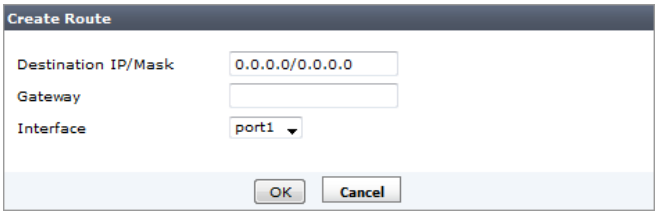
The following information and options are available:

Delete	Select the check box next to the route number and select Delete to remove the route from the table.
Create New	Select *Create New* to add a new route. See "To add a static route:" on page 73. Select the route number to edit the settings.
ID	The route number.
IP/Netmask	The destination IP address and network mask 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.

To add a static route:

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

Figure 35: Create new route



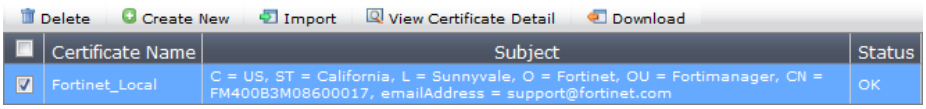
Configure the following settings:

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

Managing certificates

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

Figure 36: Local certificates window



Creating a local certificate

To create a local certificate see the following instructions.

To create a certificate request:

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

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

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

Importing certificates

To import a certificate see the following instructions.

To import a local certificate:

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

To import a CA certificate:

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

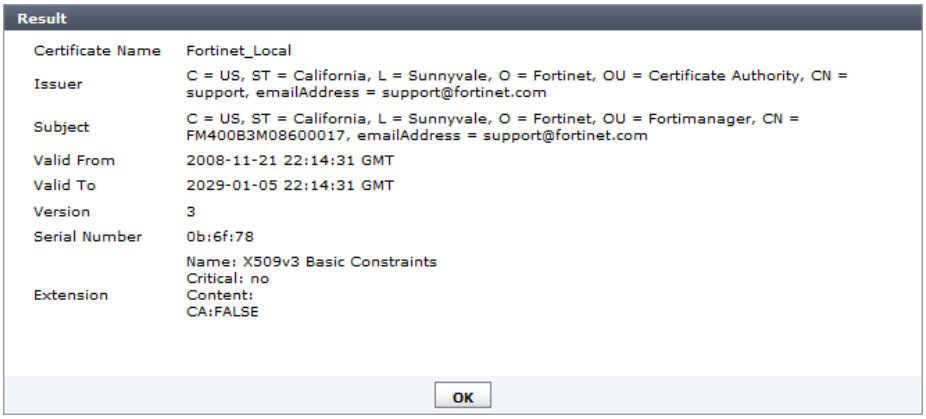
Viewing certificate details

To view certificate details see the following instructions.

To view a local certificate:

1. Go to *System* > *General* > *Certificates* > *Local Certificates*.
2. Select the certificates which you would like to see details about and click on *View Certificate Detail*; see Figure 37.

Figure 37: Local certificate detail window



This page displays the following information:

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

To view a CA certificate:

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

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

Downloading a certificate

To download a certificate see the following instructions.

To download a local certificate:

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

To download a CA certificate:

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

Configuring 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.

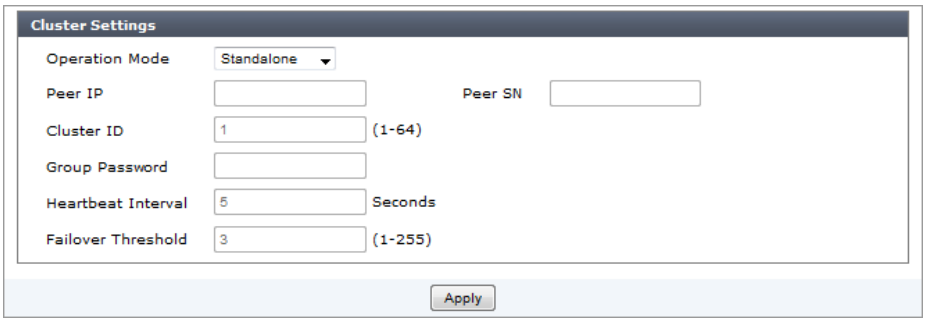
This section includes the following topics:

- Configuring HA options

Configuring HA options

To configure HA options go to *System Settings* > *General* > *HA*. From here you can configure FortiManager units to start an HA cluster or you can change the HA configuration of the cluster.

Figure 38: Cluster settings dialog box



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

When changing the HA mode for a FortiManager unit in an HA cluster, the FortiManager unit must be rebooted.

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

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

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

Configure the following settings:

Operation Mode	Select *Master* to configure the FortiManager unit to be the primary unit in a cluster. Select *Slave* to configure the FortiManager unit to be a backup unit in a cluster. Select *Standalone* to stop operating in HA mode.
Peer IP	Enter the IP address of another FortiManager unit in the cluster. For the primary unit you can add up to four Peer IPs for up to four backup units. For a backup unit you add the IP address of the primary unit.
Peer SN	Enter the serial number of another FortiManager unit in the cluster. For the primary unit you can add up to four Peer serial numbers for up to four backup units. For a backup unit you add the serial number of the primary unit.
Cluster ID	A number between 0 and 64 that identifies the HA cluster. All members of the HA cluster must have the same group ID. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different group ID. The FortiManager Web-based Manager browser window title changes to include the Group ID when FortiManager unit is operating in HA mode.
Group Password	A password for the HA cluster. All members of the HA cluster must have the same group password. The maximum password length is 19 characters. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different password.
Heartbeat Interval	The time in seconds that a cluster unit waits between sending heartbeat packets. The heartbeat interval is also the amount of time that a FortiManager unit waits before expecting to receive a heartbeat packet from the other cluster unit. The default heartbeat interval is 5 seconds. The heartbeat interval range is 1 to 255 seconds. You cannot configure the heartbeat interval of the backup units.
Failover Threshold	The number of heartbeat intervals that one of the cluster units waits to receive HA heartbeat packets from other cluster units before assuming that the other cluster units have failed. The default failover threshold is 3. The failover threshold range is 1 to 255. You cannot configure the failover threshold of the backup units. In most cases you do not have to change the heartbeat interval or failover threshold. The default settings mean that if the a unit fails, the failure is detected after 3 x 5 or 15 seconds; resulting in a failure detection time of 15 seconds. If the failure detection time is too short the HA cluster may detect a failure when none has occurred. For example, if the primary unit is very busy it may not respond to HA heartbeat packets in time. In this situation, the backup unit may assume that the primary unit has failed when the primary unit is actually just busy. Increase the failure detection time to prevent the backup unit from detecting a failure when none has occurred. If the failure detection time is too long, administrators will be delayed in learning that the cluster has failed. In most cases, a relatively long failure detection time will not have a major effect on operations. But if the failure detection time is too long for your network conditions, then you can reduce the heartbeat interval or failover threshold.

Managing administrators

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

Administrator	Select to configure administrative users accounts. For more information, see "Configuring administrator accounts" on page 79.
Profile	Select to set up access profiles for the administrative users. For more information, see "Managing administrator access" on page 83.
Remote Auth Server	Select to configure authentication server settings for administrative log in. For more information, see Managing remote authentication servers.
Admin Settings	Select to configure connection options for the administrator including port number, language of the Web-based Manager and idle timeout. For more information, see "Configuring global admin settings" on page 93.

This section includes the following topics:

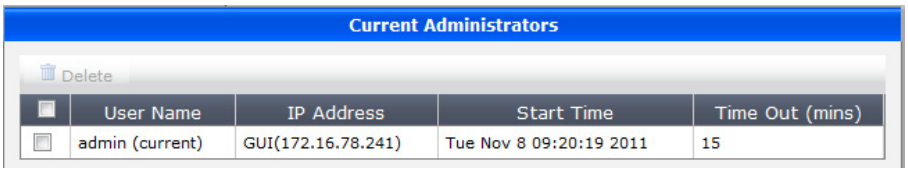
- Monitoring administrator sessions
- Configuring administrator accounts
- Managing administrator access
- Managing remote authentication servers
- Configuring global admin settings

Monitoring administrator sessions

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

To view logged in administrators on the FortiManager unit, go to *System Settings* > *General* > *Dashboard*. In the System Information widget, under *Current Administrators*, select *Detail*. The list of current administrator sessions appears; see Figure 39.

Figure 39: Administrator session list



The following information is available:

User Name	The name of the administrator account. Your session is indicated by *(current)*.
IP Address	The IP address where the administrator is logging in from.
Start Time	The date and time the administrator logged in.

Time Out (mins)	The maximum duration of the session in minutes (1 to 480 minutes).
Delete	Select the check box next to the user and select *Delete* to drop their connection to the FortiManager unit.

To disconnect an administrator:

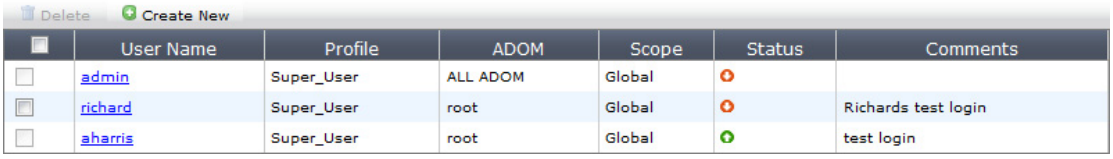
1. Go to *System Settings* > *General* > *Dashboard*.
2. In the System Information widget, under *Current Administrators*, select *Detail*. The list of current administrator sessions appears; see Figure 39.
3. Select the check box for each administrator session that you want to disconnect, and select *Delete*.
4. Select *OK* to confirm deletion of the session.

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

Configuring administrator accounts

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

Figure 40: Administrator list



The following information is available:

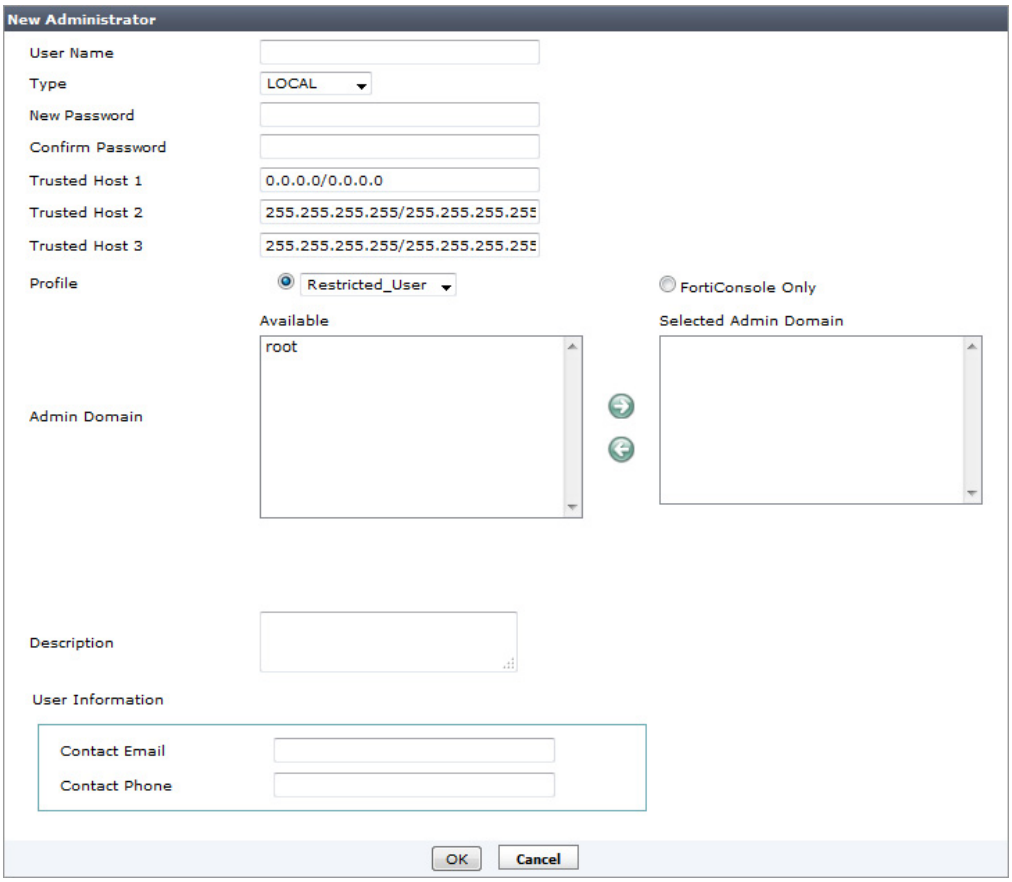
Delete	Select the check box next to the administrator you want to remove from the list and select *Delete*.
Create New	Select to create a new administrator. For more information, see "To create a new administrator account:" on page 80.
User Name	The name this administrator uses to log in. Select the administrator name to edit the administrator settings.
Profile	The administrator profile for this user that determines the privileges of this administrator. For information on administrator profiles, see "Managing administrator access" on page 83.
ADOM	The ADOM to which the administrator has been assigned.
Scope	Global

Status	Indicates whether the administrator is currently logged into the FortiManager unit not. A green circle with an up arrow indicates the administrator is logged in, a red circle with a down arrow indicates the administrator is not logged in.
Comments	Descriptive text about the administrator account.

To create a new administrator account:

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

Figure 41: Creating a new administrator account



2. Configure the following settings:

User Name	Enter the name that this administrator uses to log in. This field is available if you are creating a new administrator account.
Type	Select the type of authentication the administrator will use when logging into the FortiManager unit. If you select *LOCAL*, you will need to add a password. Otherwise, depending on the type of authentication server selected, you will select the authentication server from a drop-down list.
New Password	Enter the password. This is available if *Type* is *LOCAL*.
Confirm Password	Enter the password again to confirm it. This is available if *Type* is *LOCAL*.

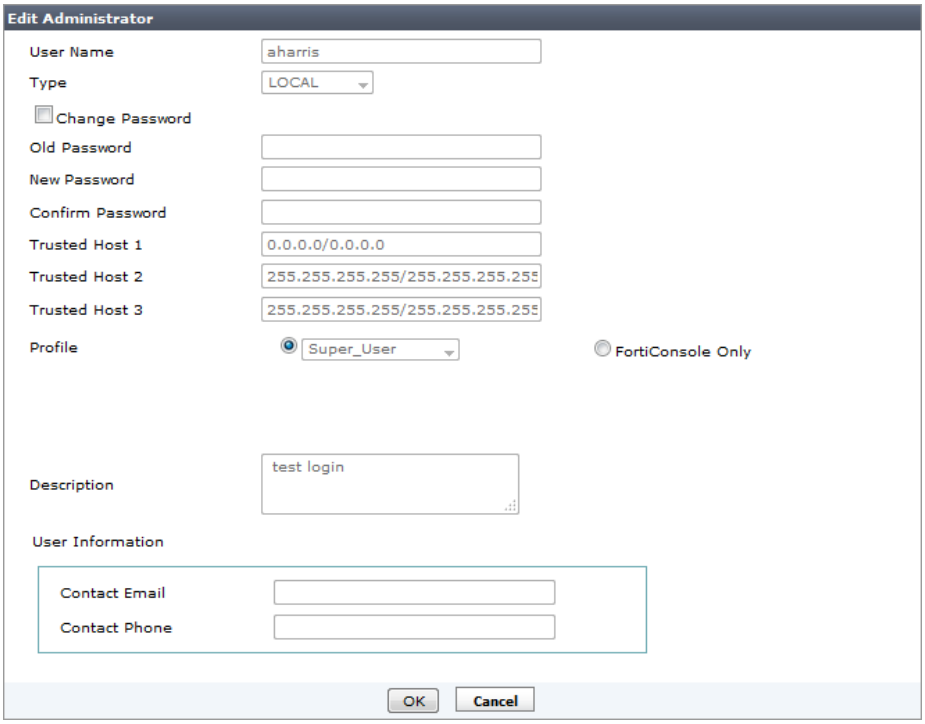
Trusted Host1 **Trusted Host2** **Trusted Host3**	Optionally, enter the trusted host IP address and network mask from which the administrator can log in to the FortiManager unit. You can specify up to three trusted hosts. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see “Using trusted hosts” on page 83.
Profile	Select a profile from the list, or select *FortiConsole Only*. The profile selected determines the administrator’s access to FortiManager unit features. To create a new profile see “Configuring administrator profiles” on page 85.
Admin Domain	Choose the ADOM this admin will belong to. This field is available only if ADOMs are enabled.
Description	Optionally, enter a description of this administrator’s role, location or reason for their account. This field adds an easy reference for the administrator account.
User Information (optional)	
Contact Email	Enter a contact email address for the new administrator.
Contact Phone	Enter a contact phone number for the new administrator.

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

To modify an existing administrator account:

1. Go to *System Settings* > *Admin*> *Administrator.* The list of configured administrators appears; see Figure 40 on page 79.
2. In the *User Name* column, double-click on the user name of the administrator you want to change. The Edit Administrator window appears; see Figure 42.

Figure 42: Editing an administrator account



3. Configure the following settings:

User Name	The name that this administrator uses to log in.
Type	The type of authentication the administrator will use when logging into the FortiManager unit. If *LOCAL* is selected, you will need to add a password. Otherwise, depending on the type of authentication server selected, you will select the authentication server from a drop-down list.
Change Password	Select to change passwords. This is available only if *Type* is *LOCAL*.
Old Password	Enter your old password. This is available only if *Type* is *LOCAL*.
New Password	Enter the password. This is available only if *Type* is *LOCAL*.
Confirm Password	Enter the password again to confirm it. This is available only if *Type* is *LOCAL*.
Trusted Host1 **Trusted Host2** **Trusted Host3**	The trusted host IP address and network mask from which the administrator logs in to the FortiManager unit. Up to three trusted hosts can be specified.
Admin Domain	The ADOM this admin belongs to. This field is available only if administrative domains are enabled.
Profile	The profile selected determines the administrator's access to FortiManager unit features. To create a new profile see "Configuring administrator profiles" on page 85.

Description	Optionally, A description of this administrator's role, location or reason for their account. This field adds an easy reference for the administrator account.
User Information (optional)	
Contact Email	A contact email address for the new administrator.
Contact Phone	A contact phone number for the new administrator.

4. Modify the settings as required. For more information about configuring account settings, see "To create a new administrator account:" on page 80.
5. Select *OK* to save your changes.

To delete an existing administrator account:

1. Go to *System Settings* > *Admin* > *Administrator.* The list of configured administrators appears; see Figure 40 on page 79.
2. Select the check box of the administrator account you want to delete and then select the *Delete* icon in the toolbar.
3. In the dialog box that appears, select *OK* to confirm the deletion.

Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. In addition to knowing the password, an administrator must connect only through the subnet or subnets you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a network mask of 255.255.255.255.

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

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

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

Managing administrator access

The *System Settings* > *Admin* > *Profile* menu enables you to create or edit administrator profiles which are used to limit administrator access privileges to devices or system features.

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

Restricted_User	Restricted user profiles have no System Privileges enabled, and have read-only access for all Device Privileges.

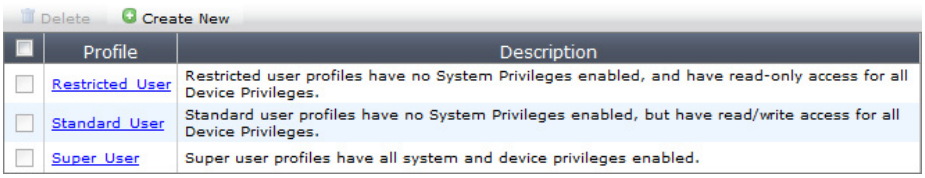
Standard_User	Standard user profiles have no System Privileges enabled, but have read/write access for all Device Privileges.
Super_User	Super user profiles have all system and device privileges enabled.

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

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

To view the list of configured administrator profiles, go to the *System Settings* > *Admin* > *Profile* page; see Figure 43.

Figure 43: Administrator profile list



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

The following information is available:

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

Configuring administrator profiles

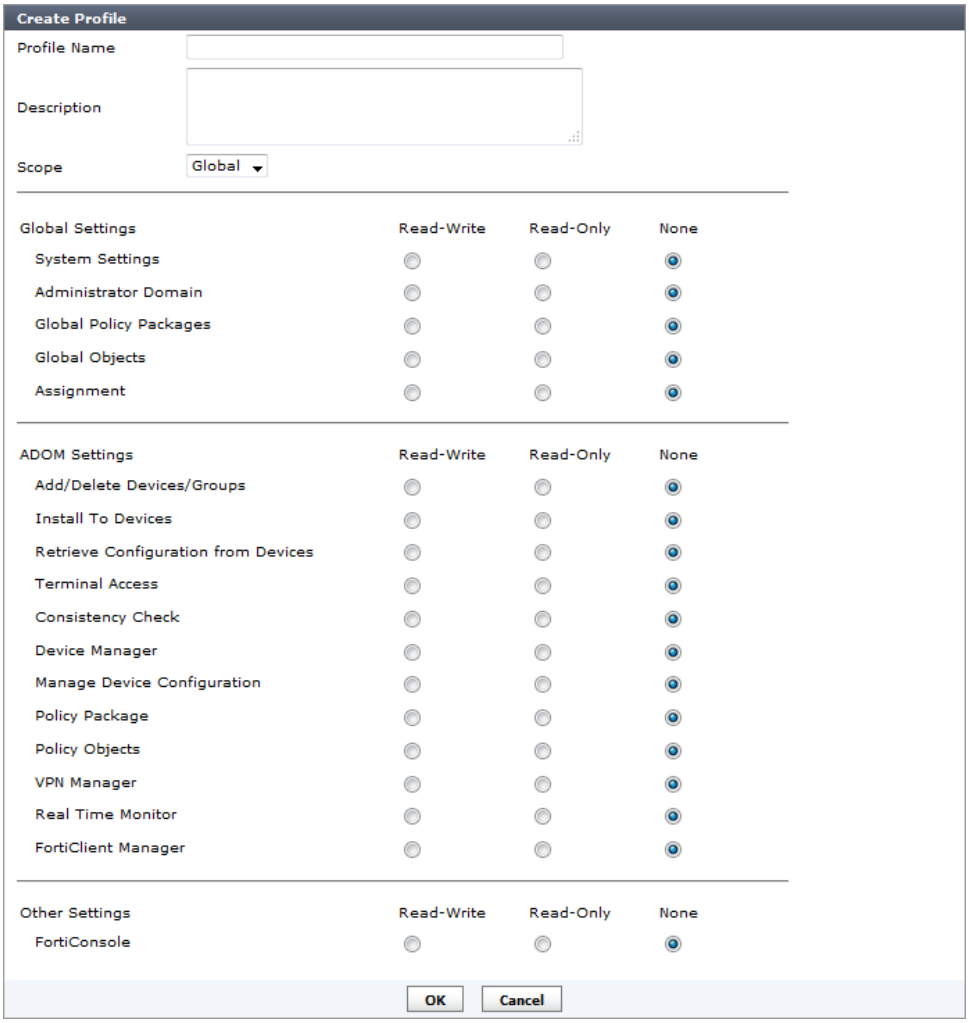
You can modify one of the pre-defined profiles or create a custom profile if needed. Only administrators with full system privileges can modify the administrator profiles.

To create a custom profile:

1. Go to *System Settings* > *Admin* > *Profile* and select *Create New*.

   The create profile dialog box appears.

   Figure 44: Create new profile dialog box



2. Configure the following settings:

Profile Name	Enter a name for this profile.
Description	Enter a description for this profile. While not a requirement, a description can help to know what the profiles is for or the levels it is set to.
Global Settings	Select *None*, *Read Only*, or *Read-Write* access for categories as required.

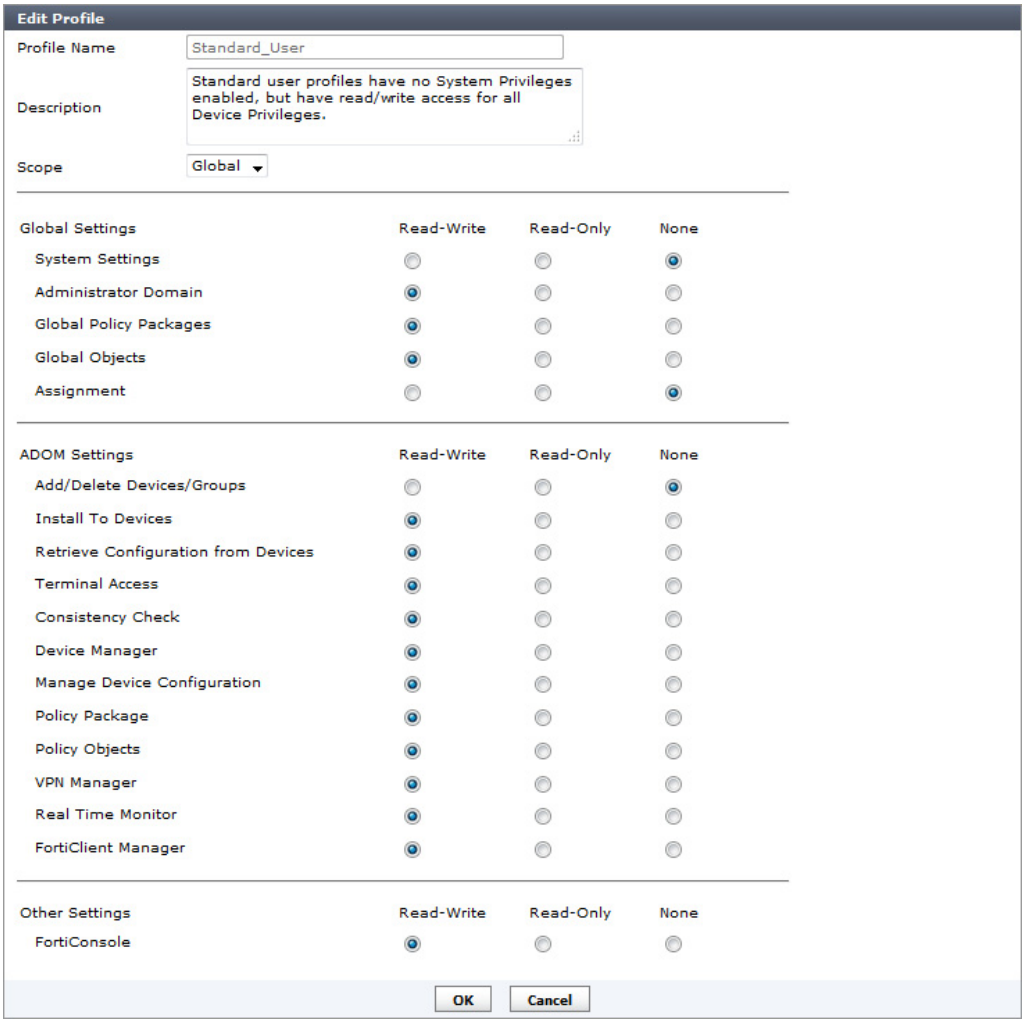
ADOM Settings	Select *None*, *Read Only*, or *Read-Write* access for categories as required.
Other Settings	Select *None*, *Read Only*, or *Read-Write* access for categories as required.

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

To modify an existing profile:

1. Go to *System Settings* > *Admin* > *Profile*. The list of available profiles appears; see Figure 43 on page 84.
2. In the *Profile* column, double-click on the name of the profile you want to change. The Edit Profile dialog box appears.

Figure 45: Edit administrator profile window



3. Configure the following settings:

Profile Name	Enter a name for this profile.
Description	Enter a description for this profile. While not a requirement, a description can help to know what the profiles is for or the levels it is set to.

Scope	Select the scope from the drop-down list.
Global Settings	Select *None*, *Read Only*, or *Read-Write* access for categories as required.
ADOM Settings	Select *None*, *Read Only*, or *Read-Write* access for categories as required.
Other Settings	Select *None*, *Read Only*, or *Read-Write* access for categories as required.

4. Configure the appropriate changes and then select *OK* to save the settings.

To delete a profile:

1. Go to *System Settings* > *Admin* > *Profile*. The list of available profiles appears; see Figure 43 on page 84.
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.

Managing remote authentication servers

The FortiManager system supports remote authentication of administrators using RADIUS, LDAP 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.

This section includes the following topics:

- Configuring RADIUS server authentication
- Configuring LDAP server authentication
- Configuring TACACS+ server authentication

Configuring RADIUS server authentication

Remote Authentication Dial-in User (RADIUS) is a user authentication and network-usage accounting system. When users connect to a server they enter a user name and password. This information is passed to a RADIUS server, which authenticates the user and authorizes access to the network.

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

Go to *System Settings* > *Admin* > *Remote Auth Server* > *Radius Server* to view the RADIUS server list.

Figure 46:RADIUS server list

The following information and options are available:

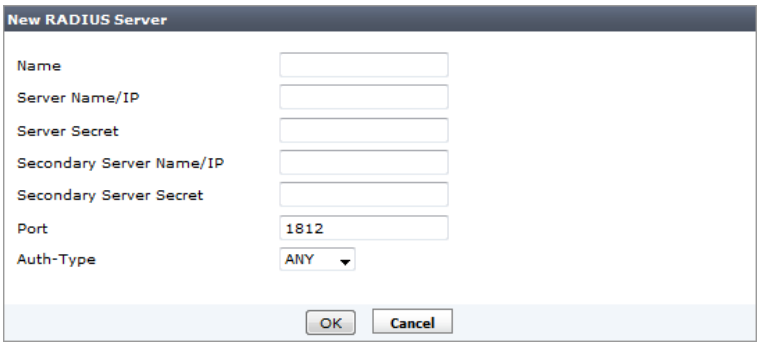
Create New	Add a new RADIUS server entry.
Delete	Select the check box next to the server entry and select *Delete*. You cannot delete a RADIUS server entry if there are administrator accounts using it.
Name	The RADIUS server name. Select the server name to edit the settings.
Server Name/IP	The IP address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

To add a RADIUS server configuration:

1. Go to *System Settings* > *Admin* > *Remote Auth Server* > *RADIUS server*. The list of configured RADIUS servers appears.
2. Select the *Create New* toolbar icon.

   The new RADIUS server dialog box appears.

   Figure 47: New RADIUS server window



3. Configure the following settings:

Name	Enter a name to identify the RADIUS server.
Server Name/IP	Enter the IP address or fully qualified domain name of the RADIUS server.
Server Secret	Enter the RADIUS server secret.
Secondary Server Name/IP	Enter the IP address or fully qualified domain name of the secondary RADIUS server.
Secondary Server Secret	Enter the secondary RADIUS server secret.

Port	Enter the port for RADIUS traffic. The default port is 1812. You can change it if necessary. Some RADIUS servers use port 1645.
Auth-Type	Enter the authentication type the RADIUS server requires. The default setting of *ANY* has the FortiManager unit try all the authentication types.

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

To modify an existing RADIUS server configuration:

1. Go to *System Settings* > *Admin* > *Remote Auth Server* > *RADIUS server*. The list of configured RADIUS servers appears.
2. In the *Name* column, select the name of the server configuration you want to change. The Edit RADIUS Server dialog box appears.
3. Modify the settings as required and select *OK* to apply your changes.

To delete an existing RADIUS server configuration:

1. Go to *System Settings* > *Admin* > *Remote Auth Server* > *RADIUS server*. The list of configured RADIUS servers appears.
2. Select the check box beside the server configuration you want to delete and then select the *Delete* toolbar icon. A confirmation dialog box appears.
3. Select *OK* to delete the server entry.

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

Configuring LDAP server authentication

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. An LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

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

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

Figure 48:LDAP server list

LDAP server list information and options:

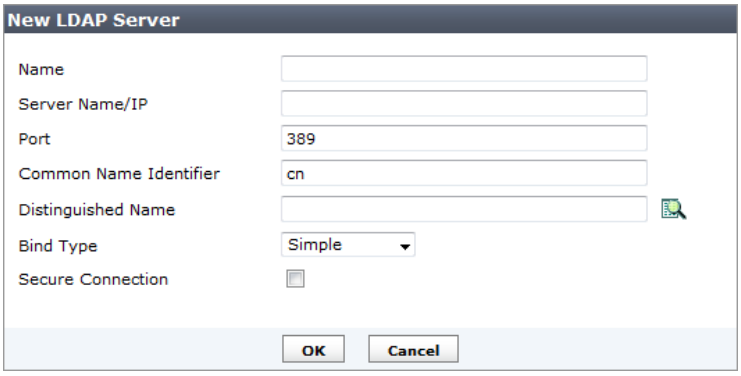
Delete	Select the check box next to the server name and select *Delete*. You cannot delete a LDAP server entry if there are administrator accounts using it.
Create New	Add a new LDAP server entry.
Name	The LDAP server name. Select the server name to edit the settings.
Server Name/IP	The IP address or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

To add a LDAP server:

1. Go to *System Settings* > *Admin* > *Remote Auth Server* > *LDAP Server*. The list of LDAP servers appears.
2. Select the *Create New* toolbar icon.

   The new LDAP Server dialog box appears.

   Figure 49: New LDAP server dialog box



3. Configure the following information:

Name	Enter a name to identify the LDAP server.
Server Name/IP	Enter the IP address or fully qualified domain name of the LDAP server.
Port	Enter the port for LDAP traffic. The default port is 389.
Common Name Identifier	The common name identifier for the LDAP server. Most LDAP servers use cn. However, some servers use other common name identifiers such as uid.
Distinguished Name	he distinguished name used to look up entries on the LDAP servers use. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier.

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

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

To modify an existing LDAP server configuration:

1. Go to *System Settings* > *Admin* > *Remote Auth Server* > *LDAP Server*. The list of configured LDAP servers appears.
2. In the *Name* column, select the name of the server configuration you want to change. The Edit LDAP Server dialog box appears.
3. Modify the settings as required and select *OK* to apply your changes.

To delete an existing LDAP server configuration:

1. Go to *System Settings* > *Admin* > *Remote Auth Server* > *LDAP Server*. The list of configured LDAP servers appears.
2. Select the check box beside the server configuration you want to delete and then select the *Delete* toolbar icon. A confirmation dialog box appears.
3. Select *OK* to delete the server entry.

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

Configuring TACACS+ server authentication

In recent years, remote network access has shifted from terminal access to LAN access. Users connect to their corporate network (using notebooks or home PCs) with computers that use complete network connections and have the same level of access to the corporate network resources as if they were physically in the office. These connections are made through a remote access server. As remote access technology has evolved, the need for network access security has become increasingly important.

Terminal Access Controller Access-Control System (TACACS) is a remote authentication protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS allows a client to accept a user name and password and send a query to a TACACS authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies network access to the user. The default TCP port for a TACACS server is 49.

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

Go to *System Settings* > *Admin* > *Remote Auth Server* > *TACACS+ Server* to create a new TACACS+ server entry or edit an existing server entry.

TACACS+ server list information and options

Delete	Select the check box next to the server name and select *Delete*. You cannot delete a TACACS+ server entry if there are administrator accounts using it.
Create New	Add a new TACACS+ server entry.

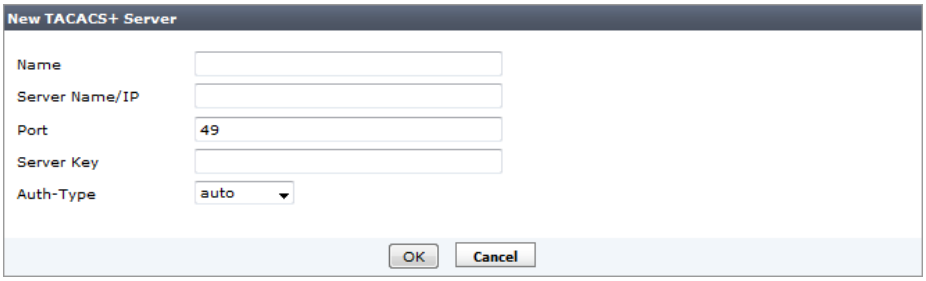
Name	The TACACS+ server name. Select the server name to edit the settings.
Server Name/IP	The IP address or DNS resolvable domain name of the TACACS+ server.

To add a TACACS+ server:

1. Go to *System Settings* > *Admin* > *Remote Auth Server* > *TACACS+ Server*. The list of TACACS+ servers appears.
2. Select the *Create New* toolbar icon.

   The new TACACS+ Server dialog box appears.

   Figure 50: New TACACS+ server dialog box



3. Configure the following information:

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

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

To modify an existing TACACS+ server configuration:

1. Go to *System Settings* > *Admin* > *Remote Auth Server* > *TACACS+ Server*. The list of configured TACACS+ servers appears.
2. In the *Name* column, select the name of the server configuration you want to change. The Edit TACACS+ Server dialog box appears.
3. Modify the settings as required and select *OK* to apply your changes.

To delete an existing TACACS+ server configuration:

1. Go to *System Settings* > *Admin* > *Remote Auth Server* > *TACACS+ Server*. The list of configured TACACS+ servers appears.
2. Select the check box beside the server configuration you want to delete and then select the *Delete* toolbar icon. A confirmation dialog box appears.
3. Select *OK* to delete the server entry. Note: You cannot delete a TACACS+ server entry if there are administrator accounts using it.

Configuring global admin settings

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

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

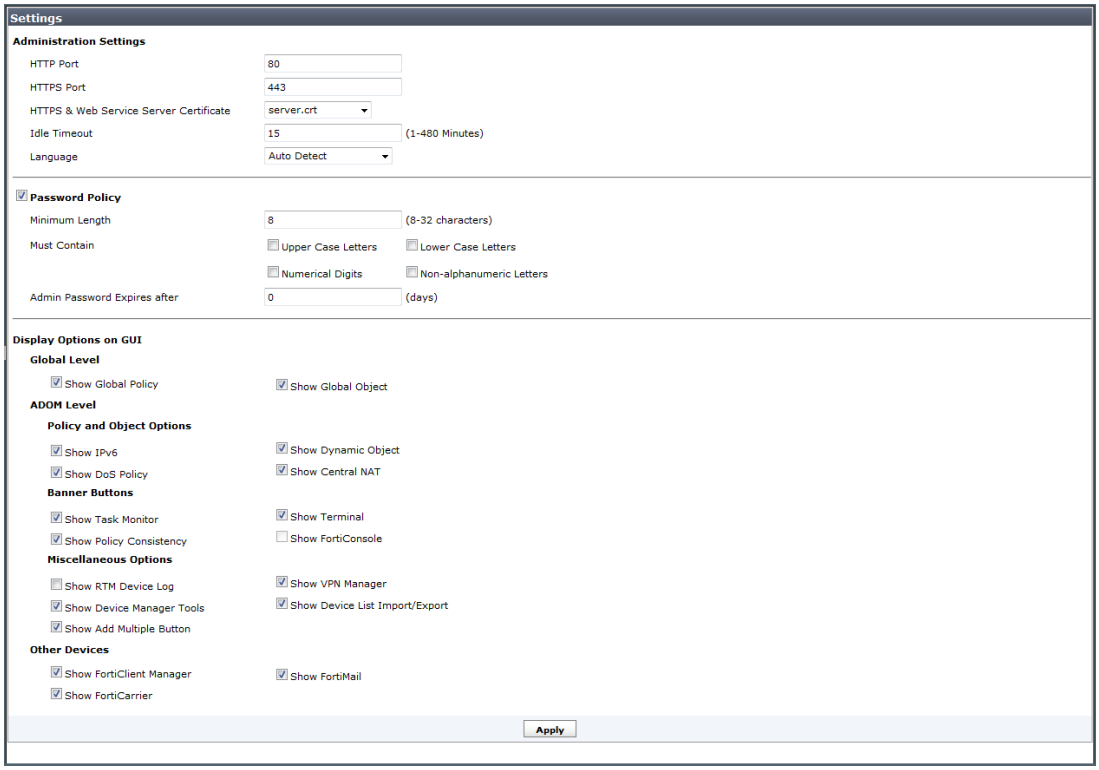
Only the `admin` administrator can configure these system options, which apply to all administrators logging onto the FortiManager unit.

To configure the administrative settings:

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

   The settings dialog box appears.

   Figure 51: Administrative settings dialog box



2. Configure the following information:

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

Idle Timeout	Enter the number of minutes that an administrative connection can be idle before the administrator must log in again. The maximum is 480 minutes (8 hours). To ensure security, the idle timeout should be a short period of time to avoid the administrator inadvertently leaving the management computer logged in to the FortiManager unit and opening the possibility of someone walking up and modifying the network options.
Language	Select a language from the drop-down list.
Password Policy	
Enable	Select to enable administrator passwords.
Minimum Length	Select the minimum length for a password. The default is eight characters.
Must Contain	Select the types of characters that a password must contain.
Admin Password Expires after	Select the number of days that a password is valid for, after which time it must be changed.
Display Settings	
Global Level	Select whether or not global policy settings and global object settings are shown.
ADOM Level	
Policy and Object Options	Select the required options from the list.
Banner Buttons	Select the required options from the list.
Miscellaneous Options	Select the required options from the list.
Other Devices	Select whether *FortiClient Manager* settings are shown.

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

Managing FortiGuard Services

The FortiGuard Center, located in *System Settings* > *FortiGuard Center* menu provides a central location for configuring and enabling your FortiManager system's built-in FDS as an FDN override server.

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

The *System Settings* > *FortiGuard Center* menu provides options that enable you configure the FortiGuard services provided by the FortiManager unit.

The following options are available:

Configuration	Select to configure override servers.
Update Mode	Select to configure the FortiGuard update management mode.
Firmware Images	Select to view the available firmware images for managed devices, and download firmware images for loading onto the managed devices. For more information see “Downloading firmware images” on page 267.

For more information and configuration instructions, see “FortiGuard Services” on page 242.

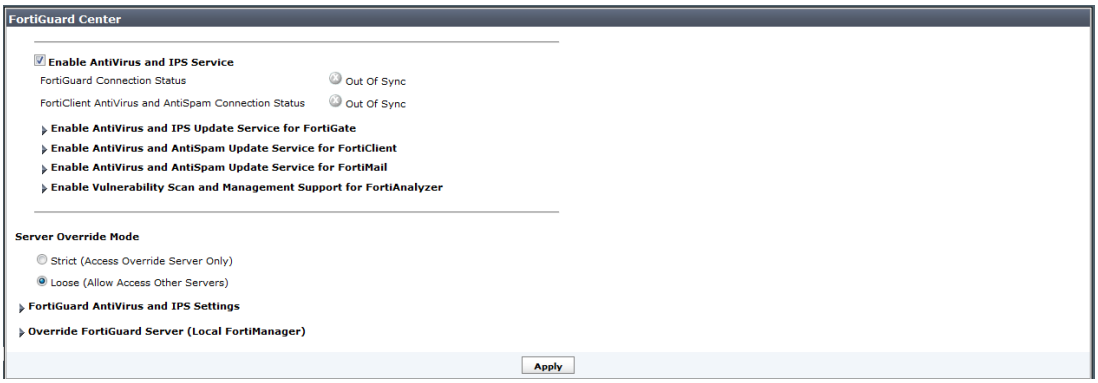
Configuring FortiGuard services

To configure FortiGuard center:

1. Go to *System Settings* > *FortiGuard Center* > *Configuration*

   The FortiGuard Center dialog appears.box.

   Figure 52: FortiGuard center dialog box



2. Configure the following settings:

Enable Antivirus and IPS Service	Select to enable antivirus and intrusion protection service.
Enable Antivirus and IPS Update Service for FortiGate	Select the OS versions from the table for updating antivirus and intrusion protection for FortiGate.
Enable Antivirus and Email Filter Update Service for FortiClient	Select the OS versions from the table for updating antivirus and email filtering for FortiClient.
Enable Antivirus and Email Filter Update Service for FortiMail	Select the OS versions from the table for updating antivirus and email filtering for FortiMail.
Enable Vulnerability Scan and Management Support for FortiAnalyzer	Select the OS versions from the table for supporting vulnerability scan and management support for FortiAnalyzer.

Server Override Mode	Select *Strict* or *Loose* override mode.
FortiGuard Antivirus and IPS Settings	
FortiGuard Distribution Network (FDN)	Select the required settings from the following options: • Enable FortiClient Service; enter port number if selected • Use Override Service Address for FortiClient • Use Override Service Address for FortiGate/FortiMail • Allow Push Update; enter IP address and port if selected • Use Web Proxy; enter IP address, port, user name, and password is selected • Schedule Regular Updates; enter the update frequency if selected. Click *Update* to apply the changes.
Advanced	Select whether or not Update Entries from FDS Server and Update Histories for Each FortiGate are logged.
Override FortiGuard Server (Local FortiManager)	
Additional Number of Private FortiGuard Servers	Click on the plus icon on the right side of the column to add additional private servers. Enter the IP address and selected the time zone of the private server to be added.
Select to enable antivirus and intrusion protection update service for private servers.	
Select to allow FortiGates to access public FortiGuard servers when private serves are unavailable.	

3. Select *Apply* to save your settings.

For more information and configuration instructions, see “FortiGuard Services” on page 242.

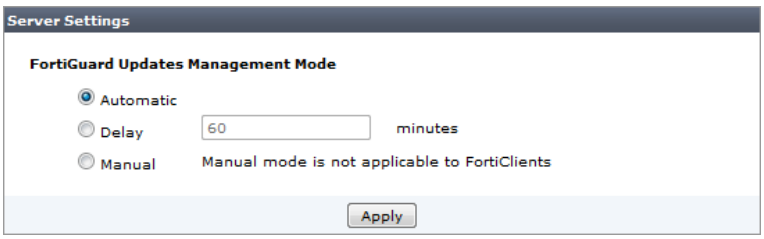
Configuring FortiGuard updates

To configure FortiGuard updates see the following instructions.

To configure FortiGuard updates:

1. Go to *System Settings* > *FortiGuard Center* > *Update Mode*.
   The server settings dialog box appears.

   Figure 53: Server settings dialog box



2. Configure the FortiGuard updates management mode by selecting, *Automatic*, *Manual*, or *Delay* and entering the delay time.

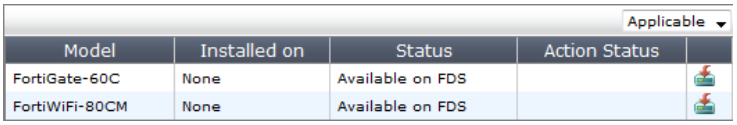
3. Select *Apply* to save your settings.

For more information and configuration instructions, see “FortiGuard Services” on page 242.

Managing firmware images

All of the loaded firmware images for all connected devices are listed under Firmware Images. The images are organized by device and version in the navigation pane. Selecting an image by going to *System Settings* > *FortiGuard Center* > *Firmware Images* and selecting the desired device and image version will display the following:

Figure 54: Firmware images list



Model	The device type and model number that the firmware is applicable to.
Installed On	The devices that the firmware is currently installed on.
Status	The status or availability, of the firmware image.
Action Status	
Download Icon	Click on the download icon to download the firmware image.

Viewing local event logs

The logs created by FortiManager are viewable within the Web-based Manager. You can use the *FortiManager v4.0 MR3 Patch Release 7 Log Message Reference*, available on the Technical Documentation web site to interpret the messages. You can view log messages in the FortiManager Web-based Manager that are stored in memory or on the internal hard disk. To view log messages stored on a FortiAnalyzer unit, you need to view them from the FortiAnalyzer Web-based Manager.

To view the log messages:

1. Go to *System Settings* > *General* > *Log Access*.
2. Select the storage location by selecting it from the *Type* drop-down list in the upper right corner.
3. Select the *Raw text*/*Formatted table* button to toggle log message view
4. Select *Refresh* to refresh the displayed logs.

Configuring advanced settings

The *System Settings* > *Advanced* menu enables you to configure mail server settings, remote output, SNMP, metafield data and other advanced settings. The following options are available:

SNMP v1/v2c	Select to configure FortiGate and FortiManager reporting through SNMP traps; see "Configuring SNMP" on page 98.
Meta Fields	Select to configure metadata fields for FortiGate objects, and for FG-5000 series shelf managers. F.
Advanced settings	Select to configure global advanced settings such as offline mode, device synchronization settings and install interface policy only; see "Configuring advanced settings" on page 108.

Configuring SNMP

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

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

Go to *System Settings* > *Advanced* > *SNMP v1/v2c* to configure your FortiManager system's SNMP settings.

The Real Time Monitor uses SNMP traps and variables to read, log, and display information from connected FortiGate devices. For more information, see "Real-time Monitor" on page 270.

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

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

This section deals only with FortiManager system generated SNMP traps, not FortiGate unit generated traps. For information on FortiGate unit generated traps, see "Real-time Monitor" on page 270.

This section provides an overview of the SNMP settings and MIB files that define the Fortinet SNMP traps and variables: It includes the following topics:

- Configuring the SNMP Agent
- Configuring an SNMP community
- Fortinet MIBs
- Fortinet traps
- Fortinet & FortiManager MIB fields

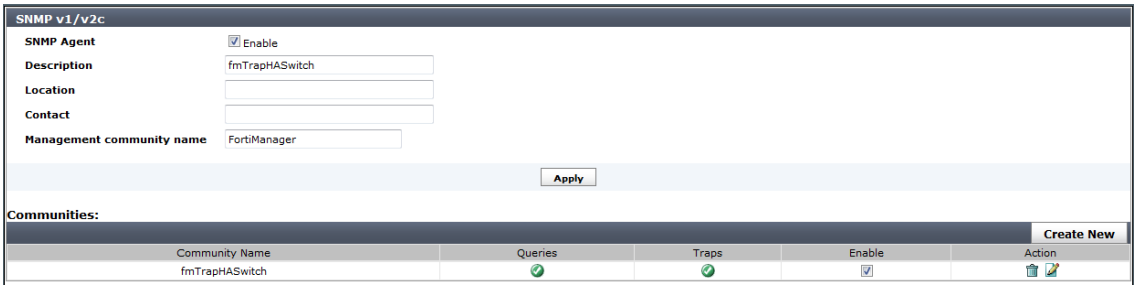
Configuring the SNMP Agent

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

Figure 55:SNMP configuration



The following information and options are available:

SNMP Agent	Select to enable the FortiManager SNMP agent. When this is enabled, it sends FortiManager SNMP traps.
Description	Enter a description of this FortiManager system to help uniquely identify this unit.
Location	Enter the location of this FortiManager system to help find it in the event it requires attention.
Contact	Enter the contact information for the person in charge of this FortiManager system.
Management Community Name	Enter the name to use for the community created by the FortiManager system during configuration of new FortiGate devices. The default value is FortiManager. This field can be a maximum of 127 characters long.

Communities	The list of SNMP communities added to the FortiManager configuration.
Create New	Select Create New to add a new SNMP community. If SNMP Agent is not selected, this control will not be visible. For more information, see “Configuring an SNMP community” on page 100.
Community Name	The name of the SNMP community.
Queries	The status of SNMP queries for each SNMP community.
Traps	The status of SNMP traps for each SNMP community.
Enable	Select to enable or unselect to disable the SNMP community.
Delete icon	Select to remove an SNMP community.
Edit icon	Select to edit an SNMP community.

Configuring an SNMP community

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

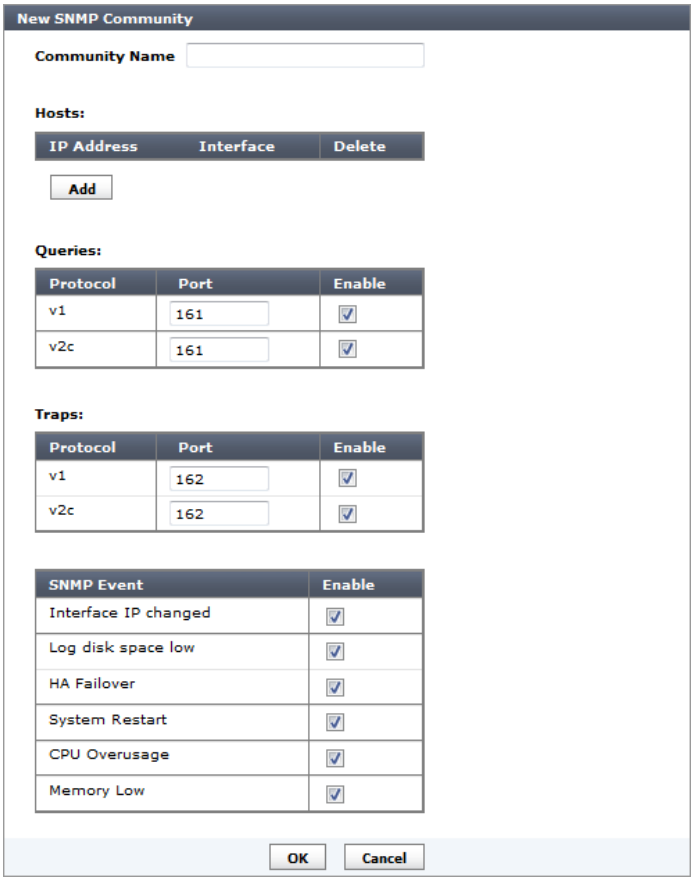
These SNMP communities do not refer to the FortiGate devices the FortiManager system is managing. For more information on FortiGate device SNMP, see either “Real-time Monitor” on page 270, or the FortiGate Administration Guide.

Each community can have a different configuration for SNMP traps and can be configured to monitor different events. You can add the IP addresses of up to 8 hosts to each community. Hosts can receive SNMP device traps, and information.

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

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

Figure 56: FortiManager SNMP community



Configure the following settings:

Community Name	Enter a name to identify the SNMP community. If you are editing an existing community, you will be unable to change the name.
Hosts	The list of FortiManager that can use the settings in this SNMP community to monitor the FortiManager system. Select Add to create a new entry that you can edit.
IP Address	Enter the IP address of an SNMP manager. By default, the IP address is 0.0.0.0, so that any SNMP manager can use this SNMP community.
Interface	Select the name of the interface that connects to the network where this SNMP manager is located. You need to do this if the SNMP manager is on the Internet or behind a router.
Delete icon	Select to remove this SNMP manager.
Add	Select to add a new default entry to the Hosts list that you can edit as needed. You can have up to 8 SNMP manager entries for a single community.
Queries	Enter the port numbers (161by default) that the FortiManager system uses to send SNMP v1 and SNMP v2c queries to the FortiManager in this community. Enable queries for each SNMP version that the FortiManager system uses.

Traps	Enter the Remote port numbers (162 remote by default) that the FortiManager system uses to send SNMP v1 and SNMP v2c traps to the FortiManager in this community. Enable traps for each SNMP version that the FortiManager system uses.
SNMP Event	Enable the events that will cause the FortiManager unit to send SNMP traps to the community. These events include: • Interface IP changed • Log disk space low • HA Failover • System Restart • CPU Overusage • Memory Low

Fortinet MIBs

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

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

The Fortinet and FortiManager MIBs are listed in Table 1 along with the two RFC MIBs. You can obtain these MIB files from Customer Service & Support. To be able to communicate with the SNMP agent, you must compile all of these MIBs into your SNMP manager. Generally your SNMP manager will be an application on your local computer.

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

Table 1: Fortinet MIBs

MIB file name or RFC	Description
FORTINET-CORE-MIB.mib	The proprietary Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor Fortinet unit configuration settings and receive traps from the Fortinet SNMP agent. For more information, see “Fortinet traps” on page 103 and “Fortinet & FortiManager MIB fields” on page 104.
FORTINET-FORTIMANAGER-MIB.mib	The proprietary FortiManager MIB includes system information and trap information for FortiManager units. For more information, see “Fortinet & FortiManager MIB fields” on page 104.

Table 1: Fortinet MIBs (continued)

MIB file name or RFC	Description
RFC-1213 (MIB II)	The Fortinet SNMP agent supports MIB II groups with the following exceptions. • No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all Fortinet traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB.
RFC-2665 (Ethernet-like MIB)	The Fortinet SNMP agent supports Ethernet-like MIB information with the following exception.
	No support for the dot3Tests and dot3Errors groups.

Fortinet traps

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

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

Table 2: Generic Fortinet traps

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

Table 3: Fortinet system traps

Trap message	Description
CPU usage high (fnTrapCpuThreshold)	CPU usage exceeds 80%. This threshold can be set in the CLI using `config system global`.
Memory low (fnTrapMemThreshold)	Memory usage exceeds 90%. This threshold can be set in the CLI using `config system global`.
Log disk too full (fnTrapLogDiskThreshold)	Log disk usage has exceeded the configured threshold. Only available on devices with log disks.
Temperature too high (fnTrapTempHigh)	A temperature sensor on the device has exceeded its threshold. Not all devices have thermal sensors. See manual for specifications.

Table 3: Fortinet system traps (continued)

Trap message	Description
Voltage outside acceptable range (fnTrapVoltageOutOfRange)	Power levels have fluctuated outside of normal levels. Not all devices have voltage monitoring instrumentation.
Power supply failure (fnTrapPowerSupplyFailure)	Power supply failure detected. Not available on all models. Available on some devices which support redundant power supplies.
Interface IP change (fnTrapIpChange)	The IP address for an interface has changed. The trap message includes the name of the interface, the new IP address and the serial number of the Fortinet unit. You can use this trap to track interface IP address changes for interfaces with dynamic IP addresses set using DHCP or PPPoE.

Table 4: FortiManager HA traps

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

Fortinet & FortiManager MIB fields

The Fortinet MIB contains fields reporting current Fortinet unit status information. The tables below list the names of the MIB fields and describe the status information available for each one. You can view more details about the information available from all Fortinet MIB fields by compiling the fortinet.3.00.mib file into your SNMP manager and browsing the Fortinet MIB fields.

Table 5: System MIB fields

MIB field	Description
fnSysSerial	Fortinet unit serial number.

Table 6: Administrator accounts

MIB field	Description	
fnAdminNumber	The number of administrators on the Fortinet unit.	
fnAdminTable	Table of administrators.	
	fnAdminIndex	Administrator account index number.
	fnAdminName	The user name of the administrator account.
	fnAdminAddr	An address of a trusted host or subnet from which this administrator account can be used.
	fnAdminMask	The network mask for fnAdminAddr.

Table 7: Custom messages

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

Table 8: FortiManager MIB fields and traps

MIB field	Description
fmModel	A table of all FortiManager models including: • fmg100 - FortiManager model 100 • fmg400 - FortiManager model 400 • fm400A - FortiManager model 400A • fm2000XL - FortiManager model 2000 • fmg3000 - FortiManager model 3000 • fmg3000B - FortiManager model 3000B
fmTrapHASwitch	The FortiManager HA cluster has been re-arranged. A new master has been selected and asserted.

Configuring metadata requirements

The *System Settings* > *Advanced* > *Meta Fields* menu enables you and other administrators to add extra information when configuring, adding or maintaining FortiGate units or adding new administrators. You can make the fields mandatory or optional, and set the side of the field.

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

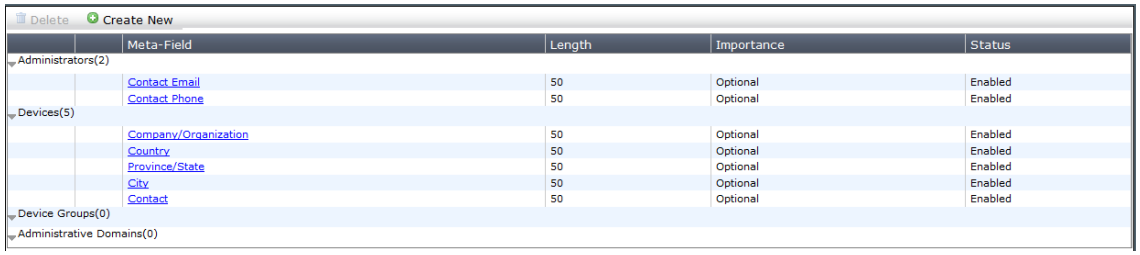
The one exception to this is the Administrators system object. This object applies only to administrators on the FortiManager unit. All other objects are related to FortiGate units.

Configuring System Metadata

Go to *System Settings* > *Advanced* > *Meta Fields* > *System Objects Meta* to add metadata fields for system-wide objects.

The list of system object metadata fields appears.

Figure 57: System objects metadata



The following information is available:

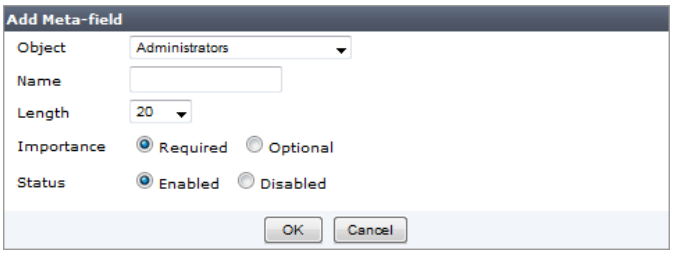
Create New **icon**	Create a new metadata field for this object.
Delete **icon**	Select to delete this metadata field.
Object	A system tab object.
Meta-Field	The name of this metadata field. Select the name to edit this field.
Length	The maximum length of this metadata field.
Importance	Indicates whether this field is required or optional.
Status	Indicates whether this field is enabled or disabled.

To add a new metadata field:

1. Go to *System Settings* > *Advanced* > *Meta Fields* > *System Objects Meta.* The list of configured system meta data objects appears; see Figure 57.
2. Select the *Create New* toolbar icon.

   The Add Meta-field dialog box appears.

   Figure 58: Add meta-field (system object)



3. Configure the following settings:

Object	The system object to which this metadata field applies.
Name	Enter the label to use for the field.
Length	Select the maximum number of characters allowed for the field.
Importance	Select *Required* to make the field compulsory, otherwise select *Optional.*
Status	Select *Disabled* to disable this field. The default is enabled.

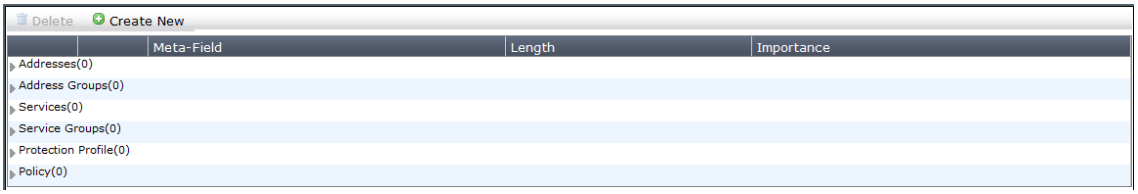
4. Select *OK* to save the new field.

Configuring FortiGate object metadata

Go to *System Settings* > *Advanced* > *Meta Fields* > *Config Objects Meta* to add metadata fields for FortiGate objects.

The list of config object metadata fields appears.

Figure 59: Config objects metadata



The following information is available:

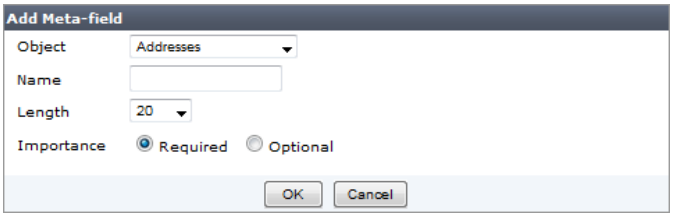
Object	A FortiGate module object.
Meta-Field	The name of this metadata field. Select the name to edit this metadata field.
Length	The maximum length of this metadata field.
Importance	Indicates whether this field is required or optional.
Create New **icon**	Create a new metadata field for this object.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

To add a new config object metadata field:

1. Go to *System Settings* > *Advanced* > *Meta Fields* > *Config Objects Meta.* The list of config object metadata fields appears; see Figure 59.
2. Select the *Create New* toolbar icon for a FortiGate object to create a new metadata field.

   The Add Meta-field dialog box appears.

Figure 60: Add meta-field (config object)



3. Configure the following settings:

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

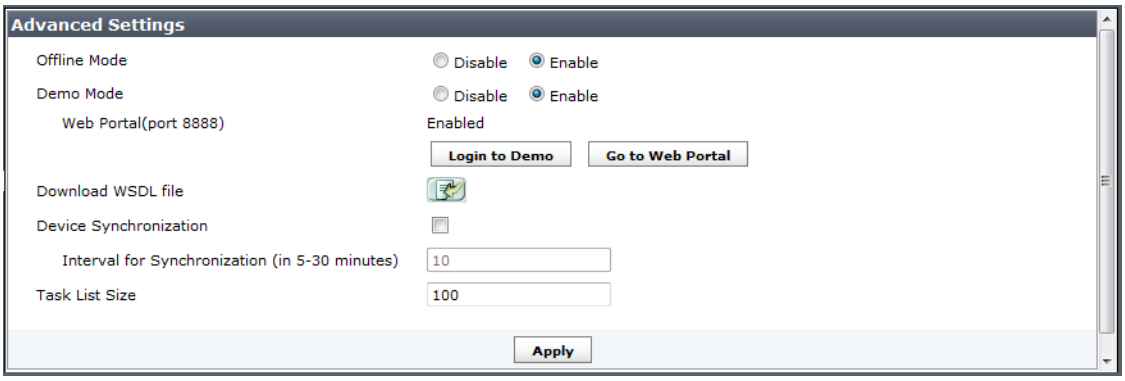
4. Select *OK* to save the new field.

Configuring advanced settings

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

The *Advanced Settings* dialog box appears.

Figure 61: Advanced settings



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.
Download WSDL file	Select to download the FortiManager unit's Web Services Description Language (WSDL) file. Web services is a standards-based, platform independent, access method for other hardware and software APIs. The file itself defines the format of commands the FortiManager will accept as well as the response to expect. Using the WSDL file, third-party or custom applications can communicate with the FortiManager unit and operate it or retrieve information just as an admin user would from the web-based manager or CLI.
Device Synchronization	Select to enable FortiManager to synchronize the settings you make with the managed devices.
Interval for synchronization	Select the time interval in minutes between synchronizations with devices.
Task List Size	Set a limit on the size of the Task List.
Verify Installation	Select to preview the installation before proceeding.
Allow Install Interface Policy Only	Select to manage and install interface based policies only instead of all device and policy configuration.

Alerts

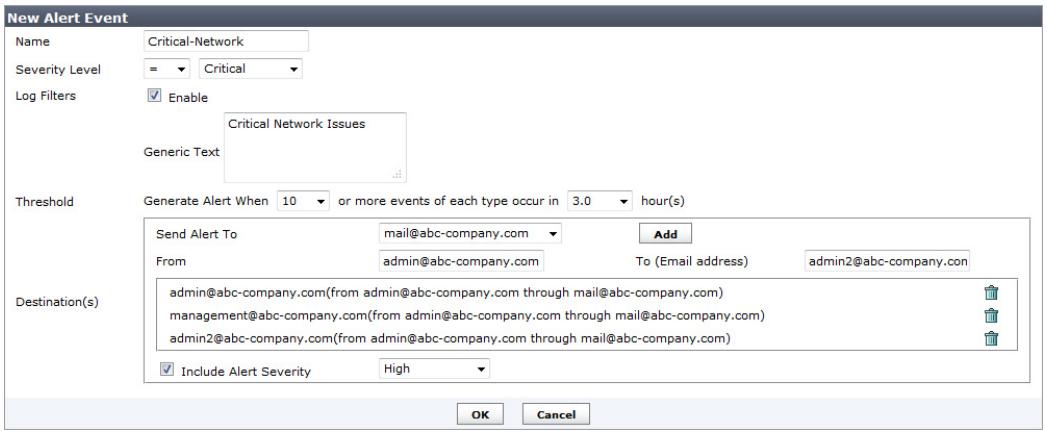
Alerts allow you to monitor and receive notification on specific activity on your network.

Alerts Event

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

Figure 62: Alert event window

Figure 63: Create new alert event window



Configure the following settings and then select *OK*:

Name	Enter a name for the alert event.
Severity Level	
Condition	Enter the conditional value: • >= • = • <=
Level	Select the severity level: • Information • Notification • Warning • Error • Critical • Alert • Emergency
Log Filters	
Enable	Select to enable log filters.
Generic Text	Optional text field.
Threshold	
Generate Alert When	Generate an alert after: • 1 • 5 • 10 • 50 • 100 or more events of each type occurs.

Occurrence	Select: • 0.5 • 1.0 • 3.0 • 6.0 • 12.0 • 24.0 • 168.0 hours.
Destination	
Send Alert To	Select: • Email Address > Create New • SNMP Server > Create New • Syslog Server > Create New
Add	Use the Add button to add multiple recipients.
Include Alert Severity	Select to include alert severity level.
Level	Select: • High • Medium High • Medium • Medium Low • Low alert severity level.

Mail Server

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

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

Figure 64: Mail server window

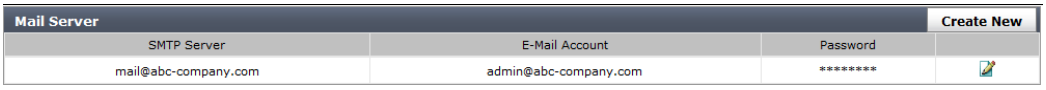
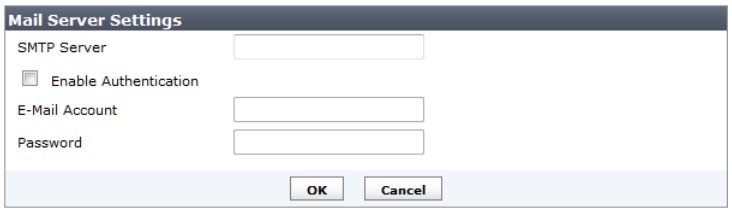


Figure 65: Mail server settings



Configure the following settings and then select *OK*:

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

Syslog Server

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

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

Figure 66: Syslog server window

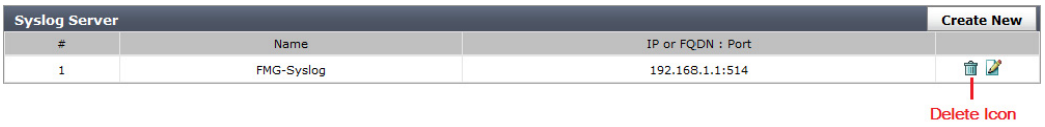
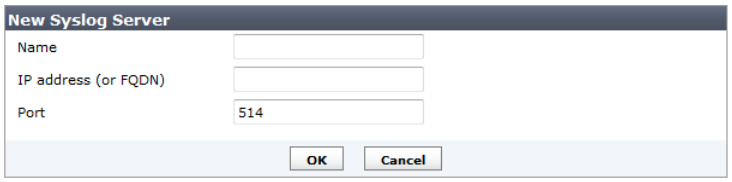


Figure 67: Syslog server settings



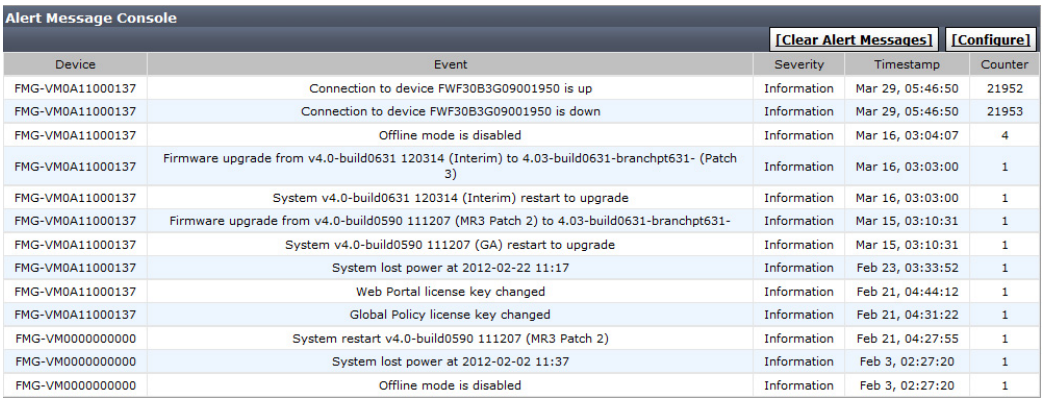
Configure the following settings and then select *OK*:

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

Alert Console

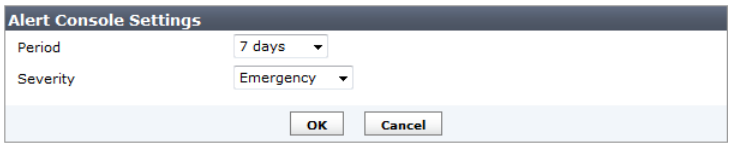
The Alert Console allows you to view alert view alert events by device. Use the Configure button to display events for a specific time frame or severity level.

Figure 68: Alert message console window



Device	Event	Severity	Timestamp	Counter
FMG-VM0A11000137	Connection to device FWF30B3G09001950 is up	Information	Mar 29, 05:46:50	21952
FMG-VM0A11000137	Connection to device FWF30B3G09001950 is down	Information	Mar 29, 05:46:50	21953
FMG-VM0A11000137	Offline mode is disabled	Information	Mar 16, 03:04:07	4
FMG-VM0A11000137	Firmware upgrade from v4.0-build0631 120314 (Interim) to 4.03-build0631-branchpt631- (Patch 3)	Information	Mar 16, 03:03:00	1
FMG-VM0A11000137	System v4.0-build0631 120314 (Interim) restart to upgrade	Information	Mar 16, 03:03:00	1
FMG-VM0A11000137	Firmware upgrade from v4.0-build0590 111207 (MR3 Patch 2) to 4.03-build0631-branchpt631-	Information	Mar 15, 03:10:31	1
FMG-VM0A11000137	System v4.0-build0590 111207 (GA) restart to upgrade	Information	Mar 15, 03:10:31	1
FMG-VM0A11000137	System lost power at 2012-02-22 11:17	Information	Feb 23, 03:33:52	1
FMG-VM0A11000137	Web Portal license key changed	Information	Feb 21, 04:44:12	1
FMG-VM0A11000137	Global Policy license key changed	Information	Feb 21, 04:31:22	1
FMG-VM0000000000	System restart v4.0-build0590 111207 (MR3 Patch 2)	Information	Feb 21, 04:27:55	1
FMG-VM0000000000	System lost power at 2012-02-02 11:37	Information	Feb 3, 02:27:20	1
FMG-VM0000000000	Offline mode is disabled	Information	Feb 3, 02:27:20	1

Figure 69: Alert console settings



Configure the following settings and then select *OK*:

Period	Select: • 1 to 7 days
Severity	Select: • Debug • Information • Notification • Warning • Error • Critical • Alert • Emergency

Device Log

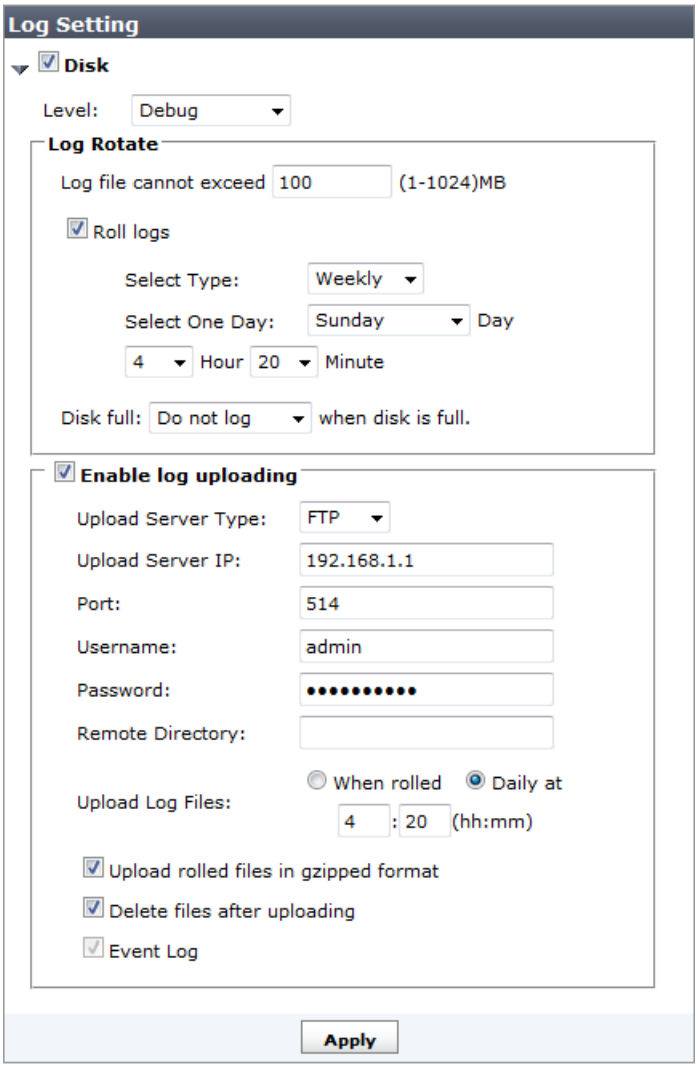
The FortiManager allow you to log system events to disk.

Log Setting

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

- Specify the severity level of logged events
- Log rotation settings
- Log upload to an FTP, SFTP or SCP server, or to a FortiAnalyzer system

Figure 70: Log setting window



Configure the following settings and then select *Apply*:

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

Log Rotate	
Log file cannot exceed	Enter the maximum log size in MegaBytes
Roll logs	Select to roll the logs. Rolling will occur either on a weekly or daily basis as selected.
Select Type	Select to roll the logs on a weekly or daily basis.
Select One Day	Select the day of the week to roll the logs. This option is enabled only when *Roll Logs* is selected and the *Type* is Weekly.
Time	Select the Hour and Minute of the day to roll the logs. The hour is based on a 24 hour clock.
Disk full	Select the action to take, *Overwritten* or *Do not log*, when the disk is full from the drop-down list.
Enable log uploading	Select to upload realtime device logs.
Upload Server Type	Select one of FTP, SFTP, SCP, or FAZ.
Upload Server IP	Enter the IP address of the upload server.
Port	Enter the port of the upload server.
Username	Select the username that will be used to connect to the upload server.
Password	Select the password that will be used to connect to the upload server.
Remote Directory	Select the remote directory on the upload server where the log will be uploaded.
When rolled	Select to upload log files when they are rolled according to settings selected under *Roll Logs*.
Daily at	Select the hour to upload the logs. The hour is based on a 24 hour clock
Upload rolled files in gzipped format	Select to gzip the logs before uploading. This will result in smaller logs, and faster upload times.
Delete files after uploading	Select to remove device log files from the FortiManager system after they have been uploaded to the Upload Server.
Event Log	This option is not available.

Log Access

Log access displays current logs and the size of the log file.

Using FortiManager Wizards

FortiManager provides you with configuration 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 two wizards:

- Add Device Wizard
- Install Wizard

This section will describe each wizard and their usage.

Using the add device wizard

The add device wizard allows you to add or import devices to you FortiManager unit.

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

The add device function allows you to quickly and easily add devices to be centrally managed by your FortiManager unit.

A shortened version of the Add Device Wizard can also be used to import policies to an already installed or imported device. See “Importing policies to a device” on page 145.

Launching the add device wizard

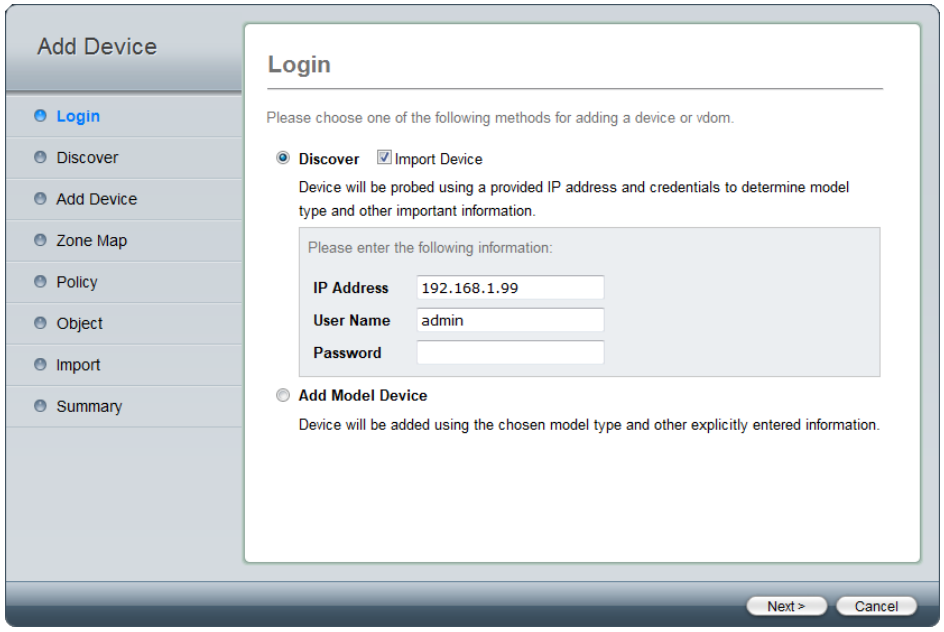
To launch the Add Device Wizard, click on the Add Device icon, located on the main toolbar. The Add Device Wizard will open; see Figure 72 below.

Figure 71: Add Device icon

The login window gives you three options for importing or adding new devices.

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.

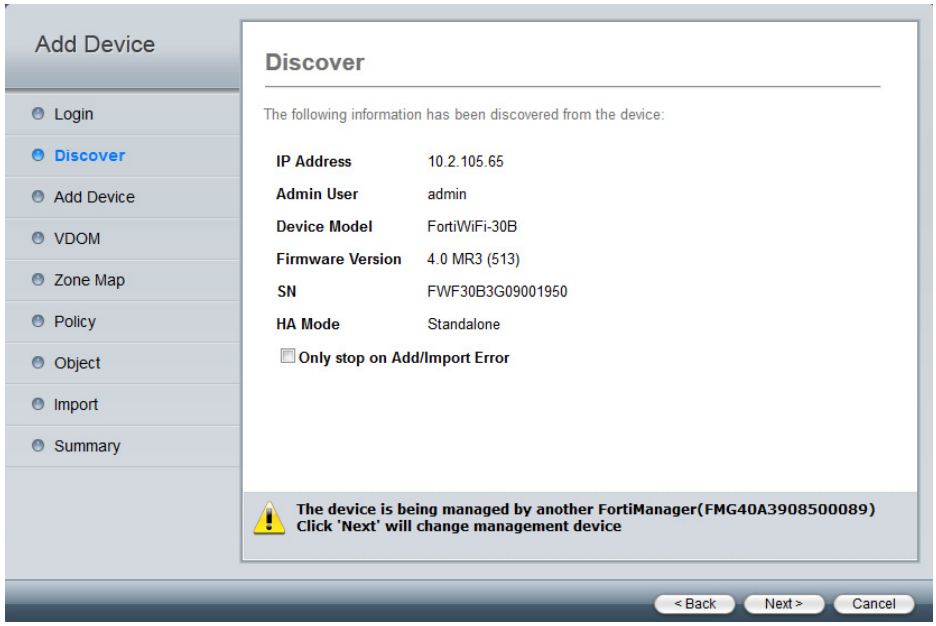
Figure 72: Add device wizard login window



Import device

This option allows you to import a device and bring all of its policies and objects into the FortiManager system. You will require the IP address of the unit you wish to import, as well as the unit's login and password. Select *Import Device* to use this method. See "Importing a device" on page 119.

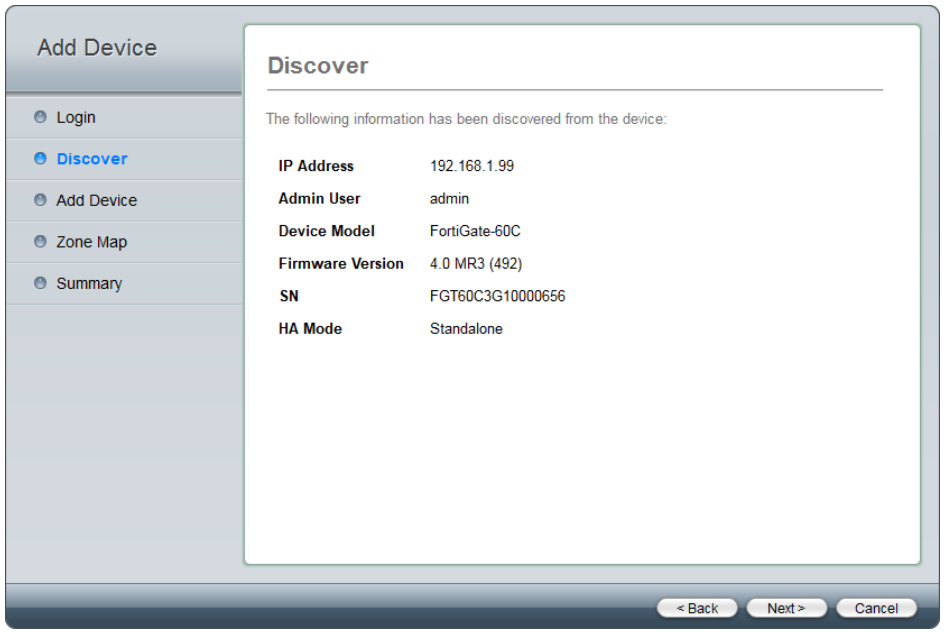
Figure 73: Import device summary window



Discover

You will require the IP address of the unit you wish to add, as well as the unit's login and password. The device is probed using the provided IP address and credentials to determine model type and other important information. See "Adding a Device" on page 123.

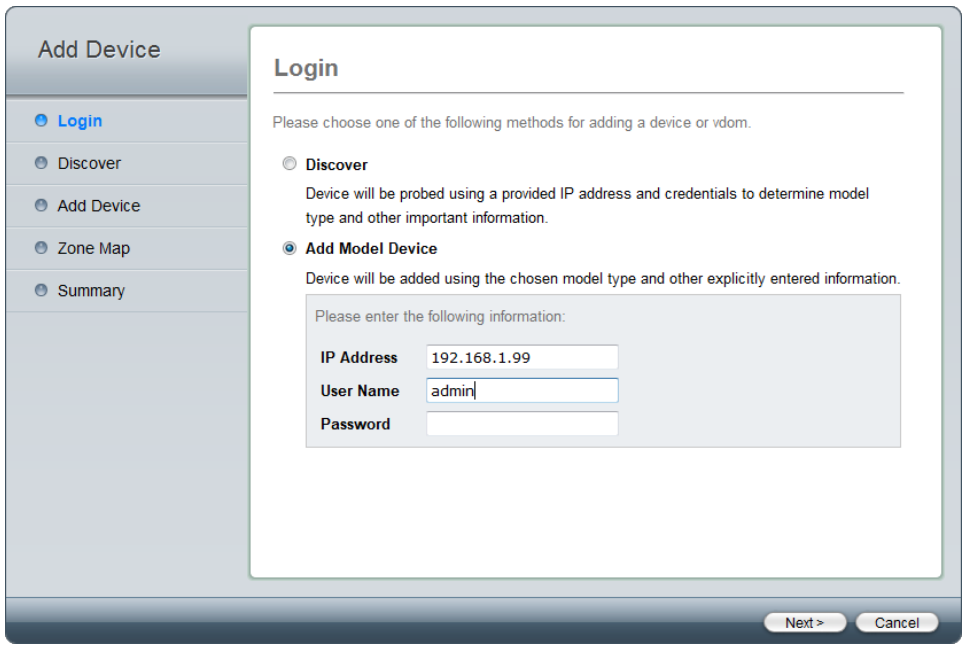
Figure 74: Discover method summary window



Add model device

If you have a new unit you wish to install, but it is not yet online, you can use this feature to add it to your FortiManager. You must have all related information about the unit to use this feature. See "Adding a Device" on page 123.

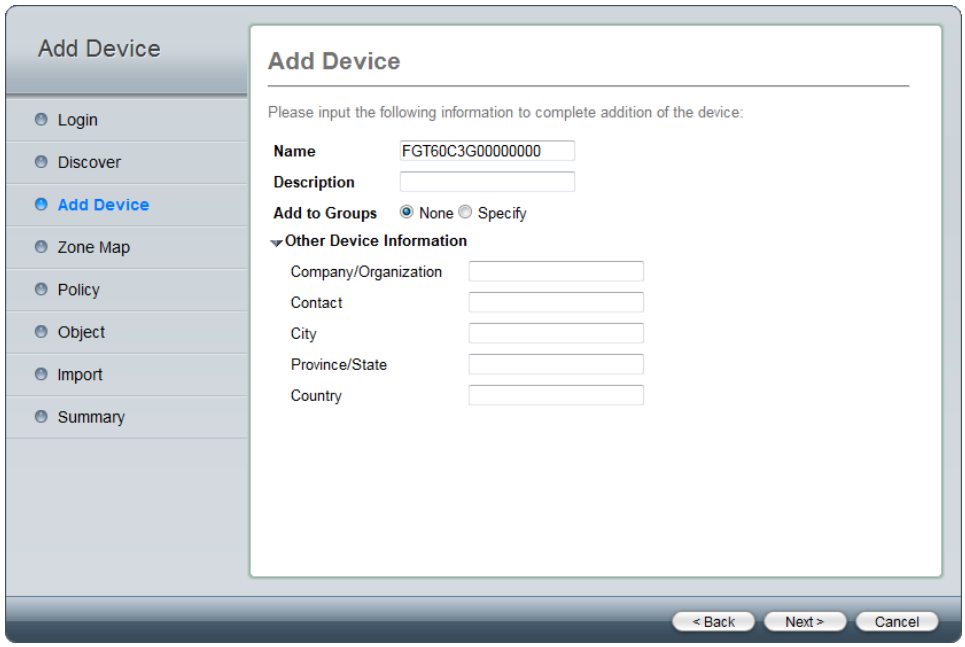
Figure 75: Add model device method window



Importing a device

This option allows you to import a device and bring all of its policies and objects into the FortiManager. You will have the opportunity to provide additional information during the process.

Figure 76: Importing device additional information window



Configure the following settings:

Name	Enter a name for the device.
Description	Enter a description of the device (optional).
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, and Country.

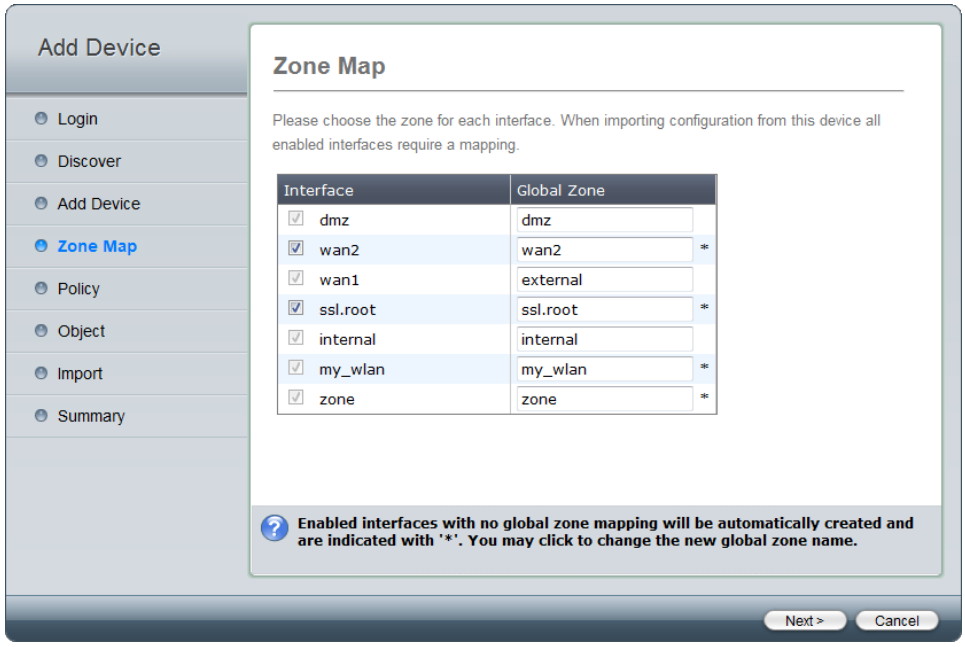
If successful, you can continue on to assigning interfaces for the device. If unsuccessful, go back and verify that the information you have entered is correct.

Global Zone Map

You can use the Global Zone Map section of the wizard to map your dynamic interface zones.

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

Figure 77: Zone map window

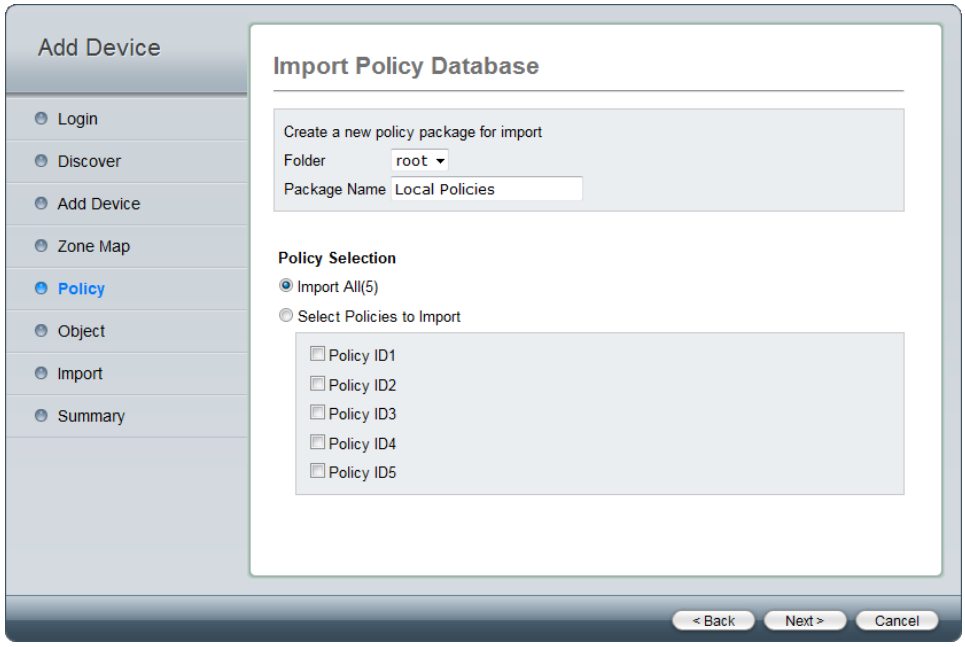


Policy

The wizard will then perform a policy search to find all policies in preparation for importation into FortiManager's database.

Once this step is complete, you will be shown a summary of the policies. Choose a folder from the drop-down list, enter a new policy package name, and select the policies you would like to import from the list.

Figure 78: Import policy summary

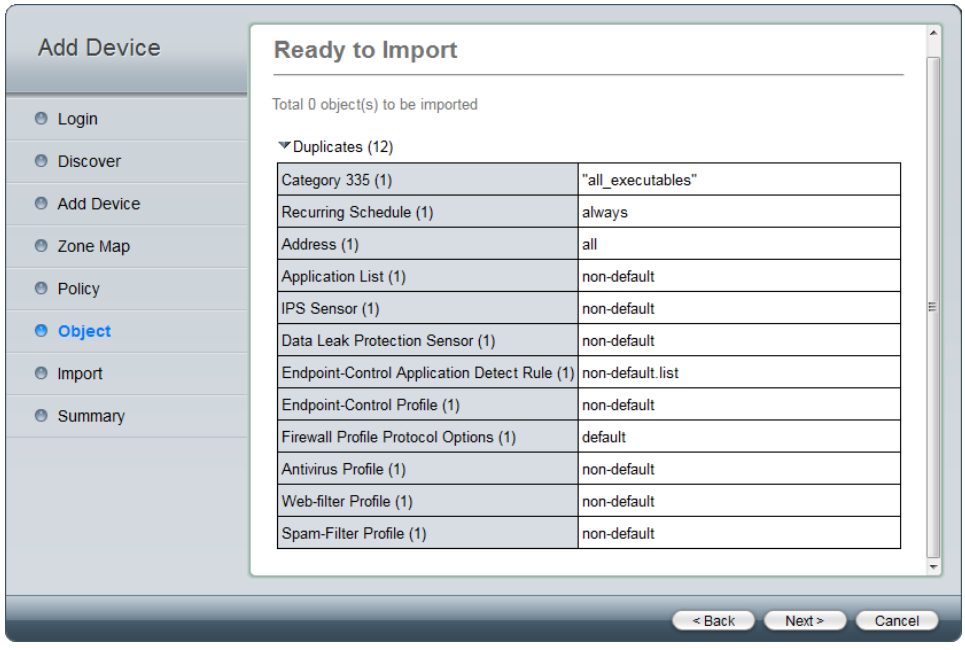


In FortiManager v4.0 MR3 Patch Release 7, Policy Selection > Select Policies to Import, you can select both IPv4 and IPv6 policies.

Object

The wizard then searches the unit for objects to import, and reports any conflicts it detects. If conflicts are detected, you can decide to overwrite the existing item, skip it, or rename it.

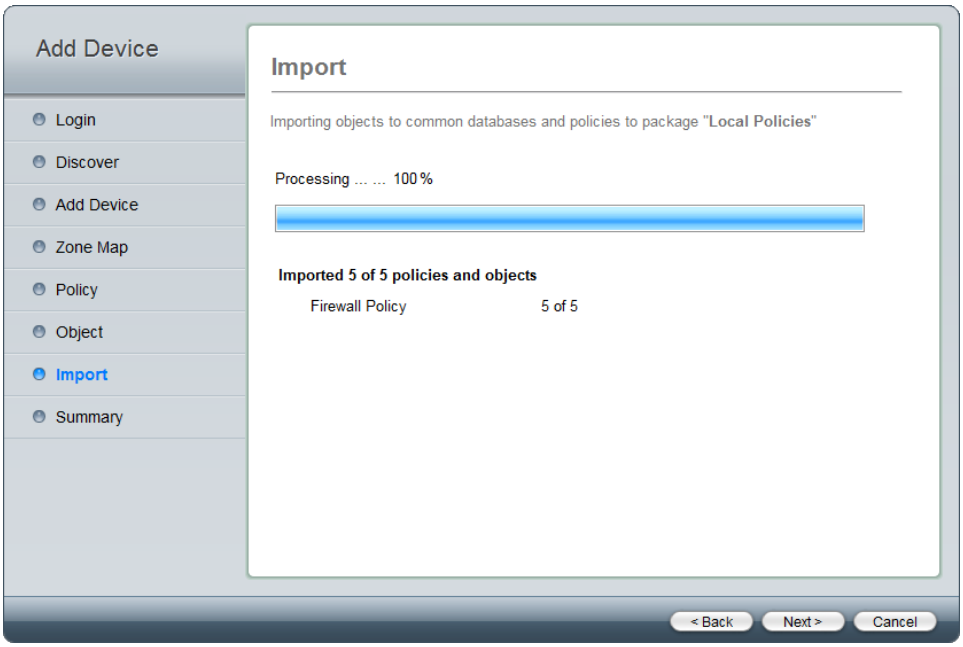
Figure 79: Import object summary



Importing into FortiManager

Once you have completed the previous steps, you will be able to start the import into FortiManager.

Figure 80: Device import successful window

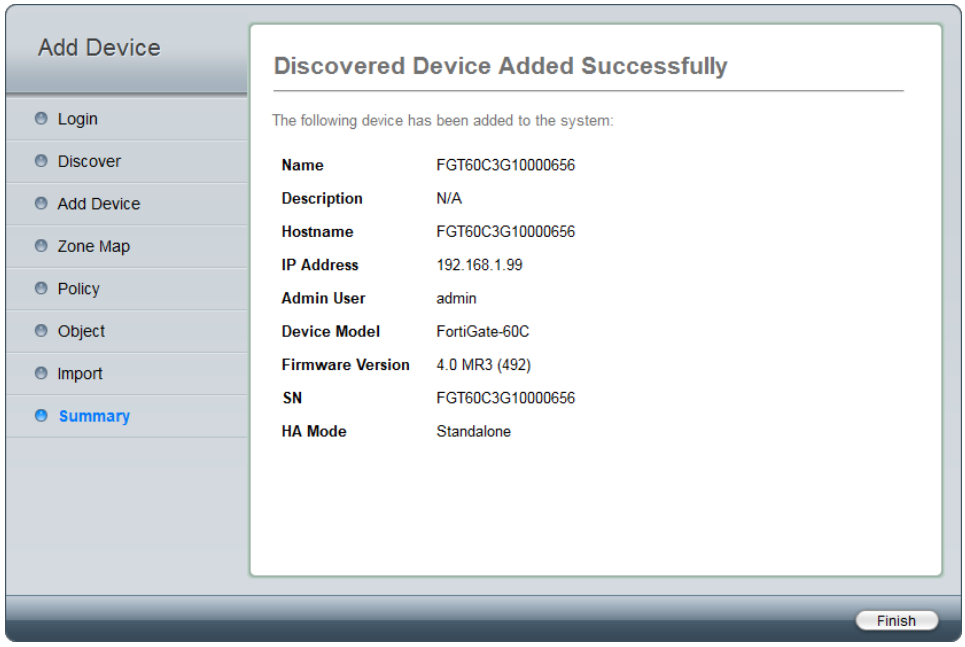


Remember: All policies are executed from the top down! Inserting imported policies into the wrong place could cause unwanted effects!

Device import summary

Once the device is successfully imported, this screen will show you a summary of your imported device.

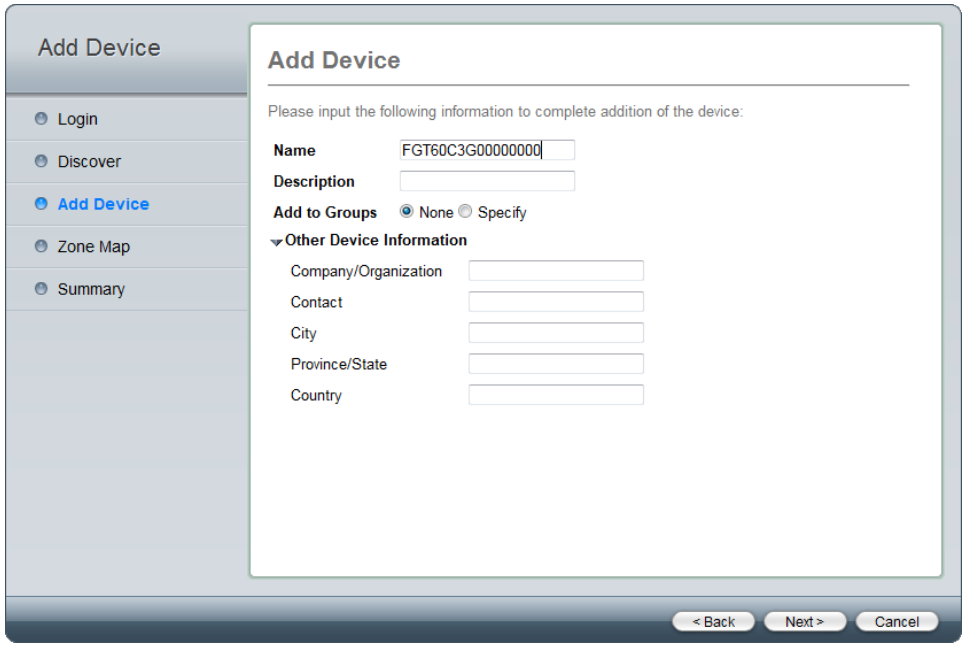
Figure 81: Import device summary window



Adding a Device

If adding a device, regardless of which feature you use, you will have the opportunity to provide additional information in the process.

Figure 82: Adding device additional information window

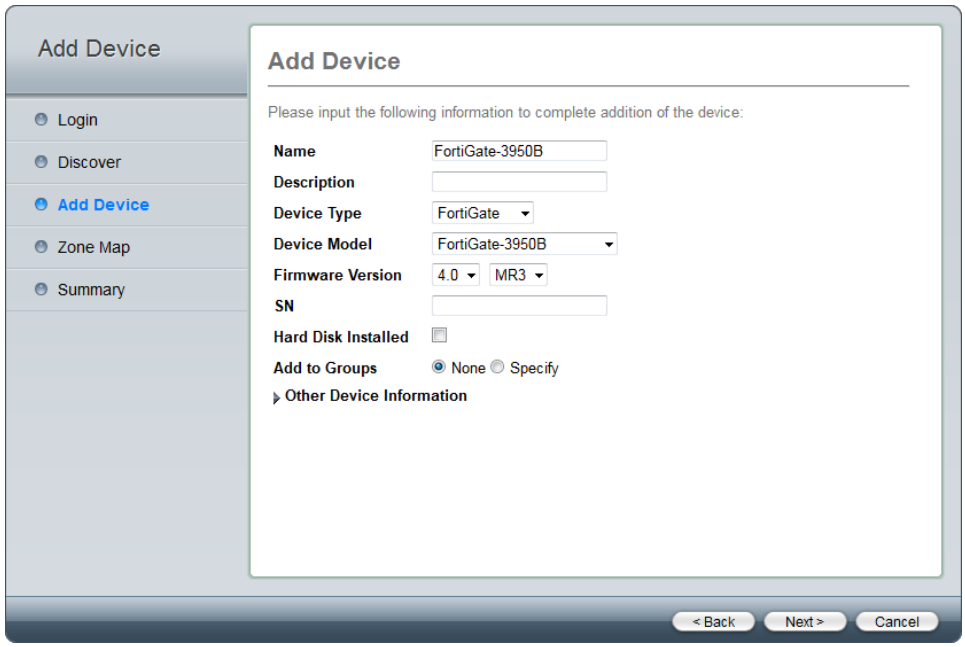


Configure the following settings:

Name	Enter a name for the device.
Description	Enter a description of the device (optional).

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, and Country.

Figure 83: Adding device model additional information window

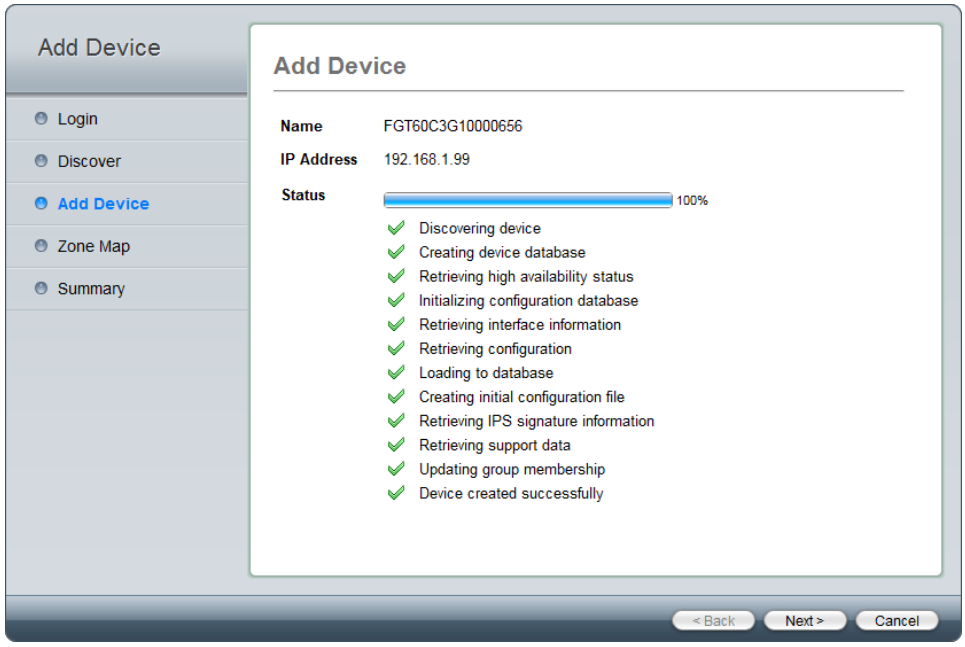


Configure the following settings:

Name	Enter a name for the device.
Description	Enter a description of the device (optional).
Device Type	Select the device type from the drop-down list.
Device Model	Select the device model from the drop-down list.
Firmware Version	Select the firmware version from the drop-down lists.
SN	Enter the serial number of the device (optional).
Hard Disk Installed	Select if there is a hard disk or hard disks installed in the device.
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, and Country.

After you add your additional information, the FortiManager will add the device or device model to the system and give you a confirmation of success or failure.

Figure 84: Confirmation of success or failure



If successful, you can continue on to assigning interfaces to the new device. If unsuccessful, go back and verify that the information you have entered is correct.

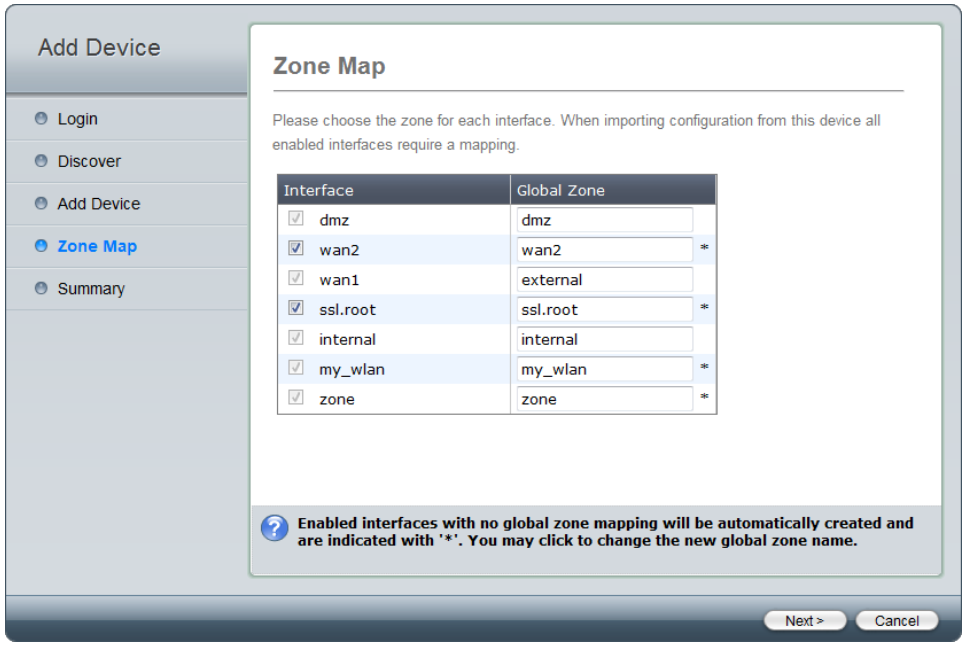
Global Zone Map

You can use the Global Zone Map section of the Wizard to map your dynamic interface zones.

If adding a new device, all of your current mappings will appear and you can choose the zones for your interfaces.

If you are adding a new device, you cannot go back from this step.

Figure 85: Zone map window



Device Summary

This screen will show you a summary of your added device.

Figure 86: Add device summary window

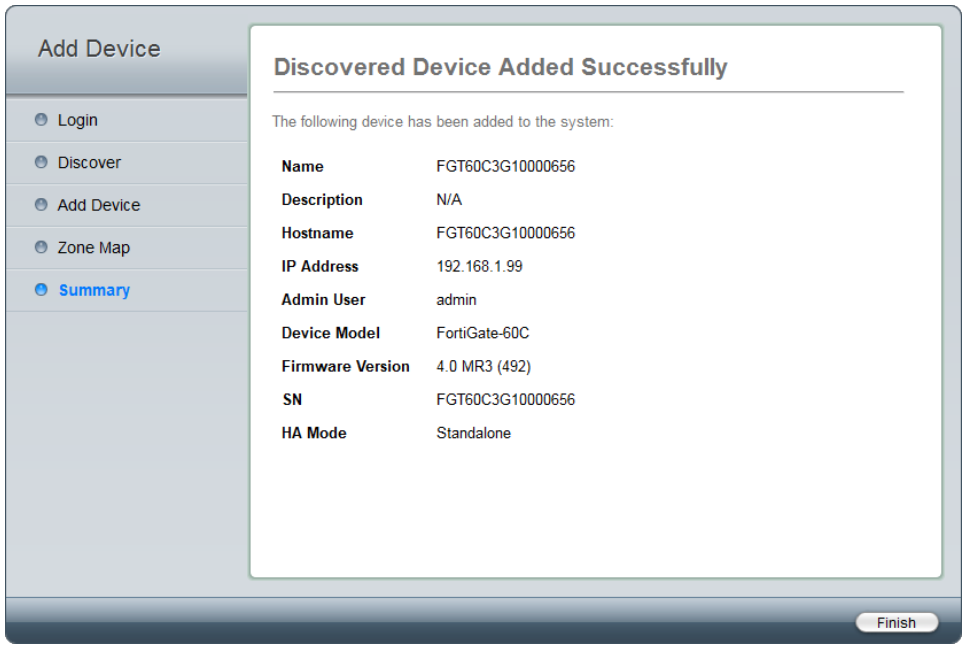
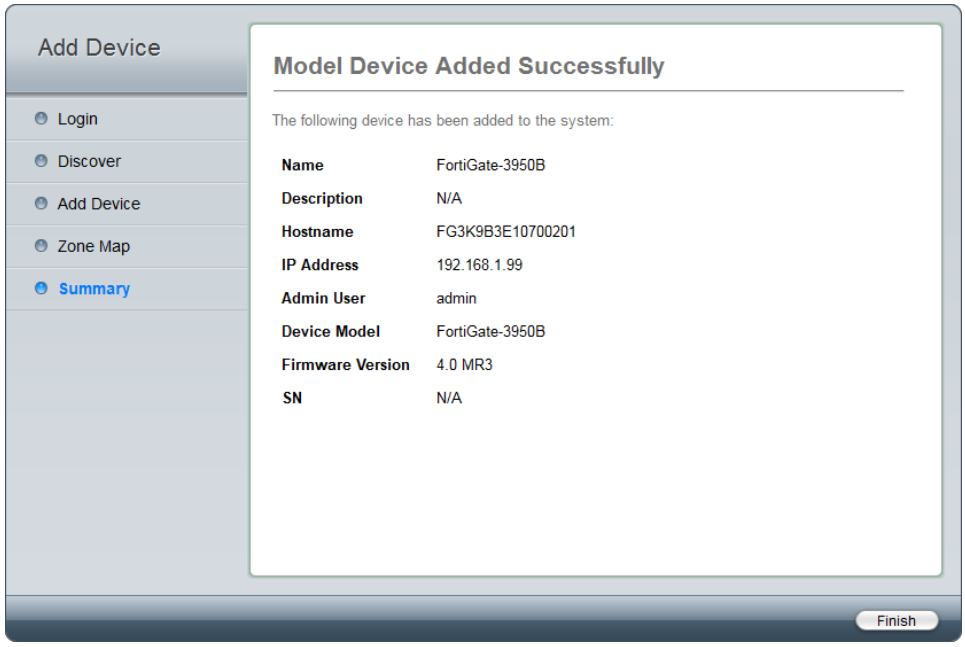


Figure 87: Add model device summary window



Using the install wizard

The Install Wizard will assist you in installing settings to one or more of your FortiGate devices.

Launching the install wizard

To launch the Install Wizard, click on the *Install* icon, located on the main toolbar. The Install Wizard will open.

Figure 88: Install icon

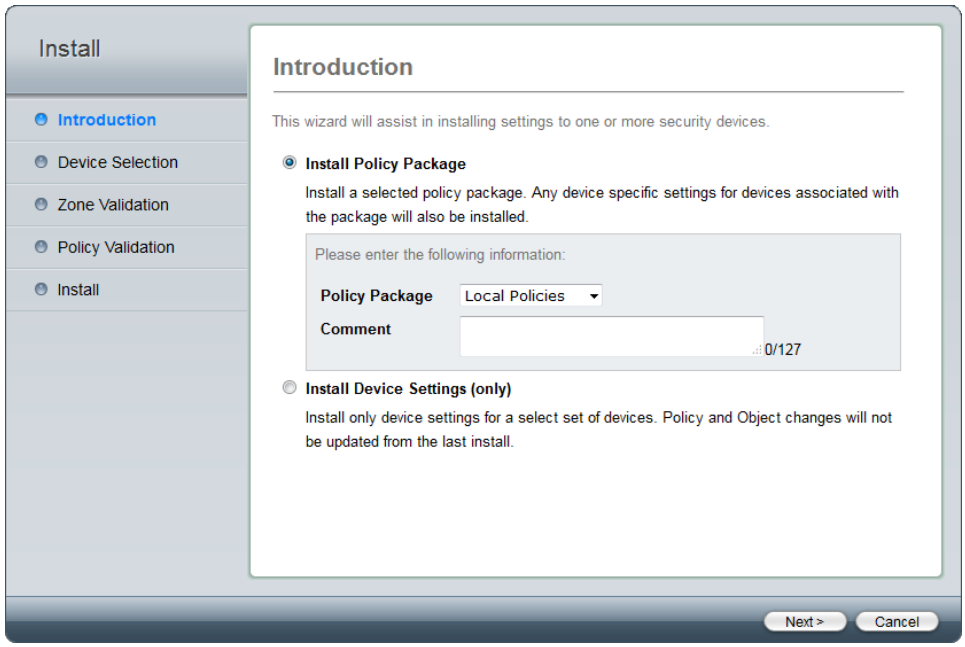
The Introduction window gives you two options for installing settings:

- *Install Policy Package*: Install a selected policy package. Any device specific settings for devices associated with package will also be included. See “Installing a policy package” below.
- *Install Device Settings (only)*: Install only device settings for a select set of devices. Policy and Object changes will not be updated from the last install. See “Installing device settings” on page 131.

Installing a policy package

Select *Install Policy Package*, select the policy package from the drop-down list, and optionally enter a comment for the policy package being installed.

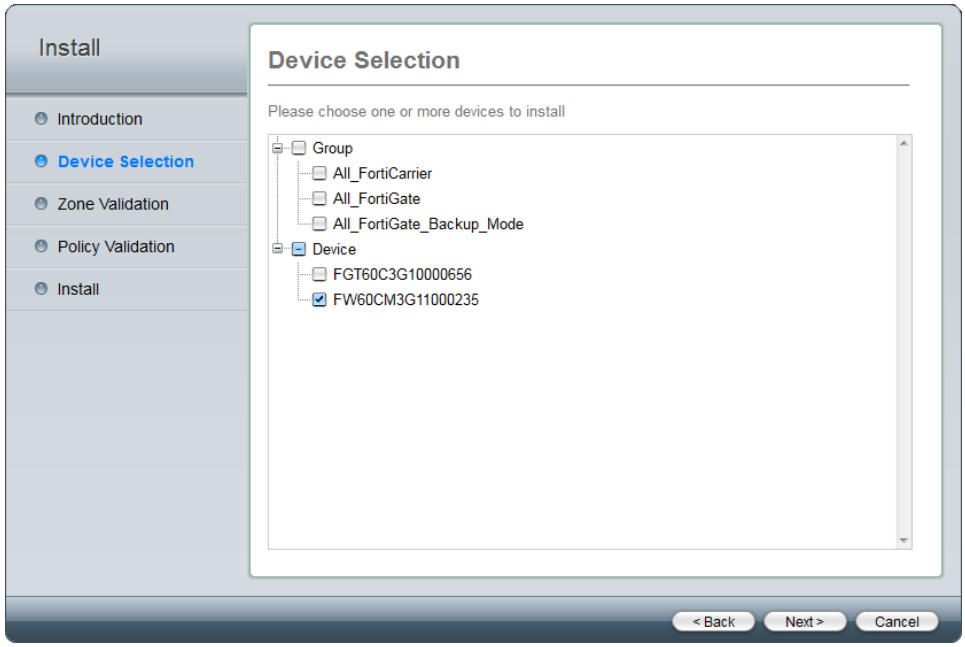
Figure 89: Install policy package



Device selection

The device selection window allows you to choose one or more devices or groups to install.

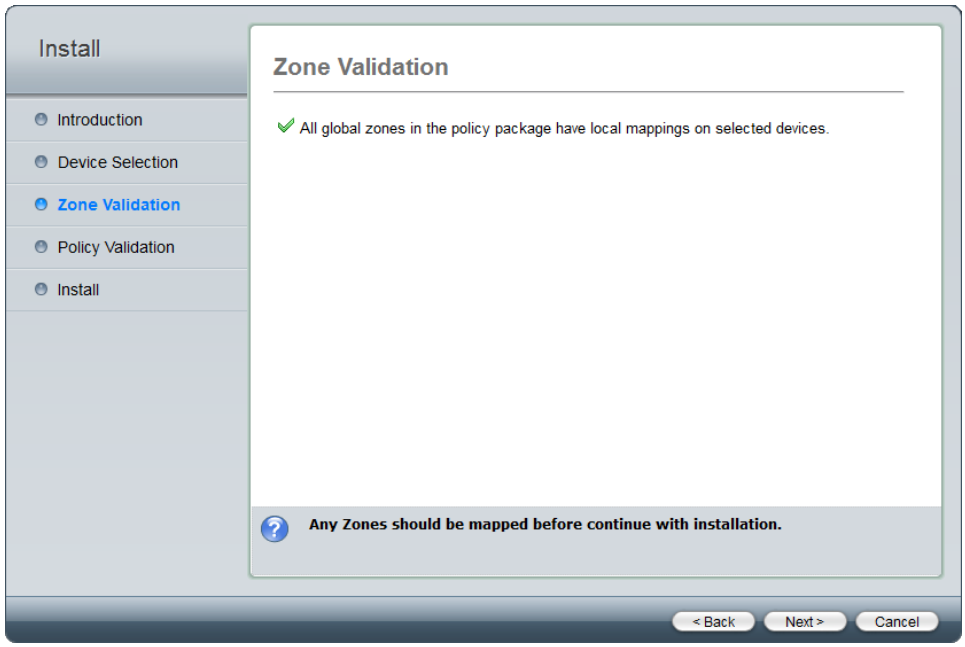
Figure 90: Policy package device selection window



Zone Validation

Zone validation checks to ensure that all global zones in the policy package have local mappings on the selected devices.

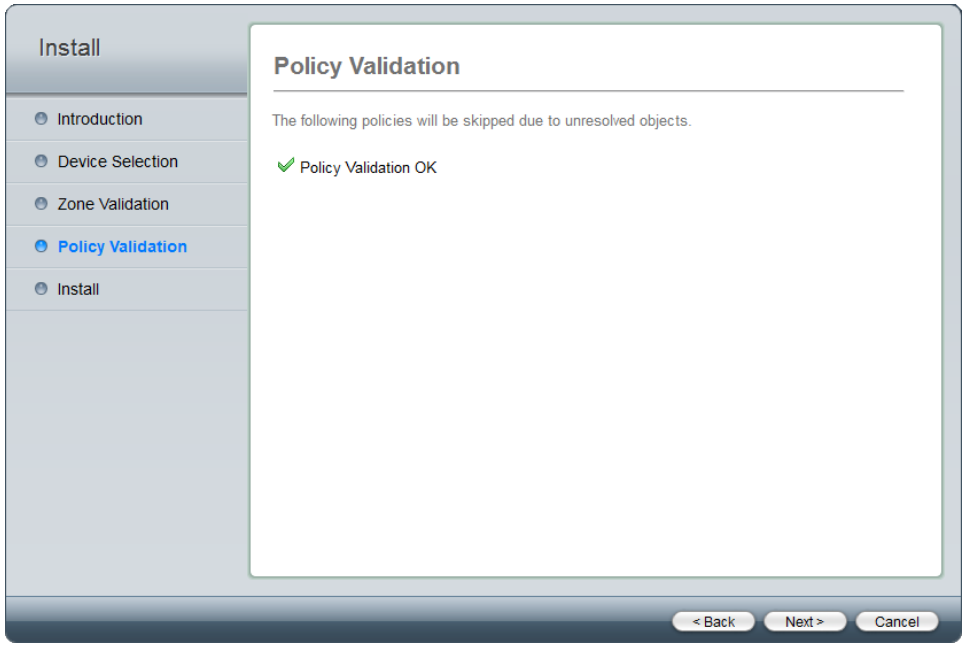
Figure 91: Policy package zone validation window



Policy validation

Policy validation checks to ensure that the policies in the policy package do not have unresolved objects.

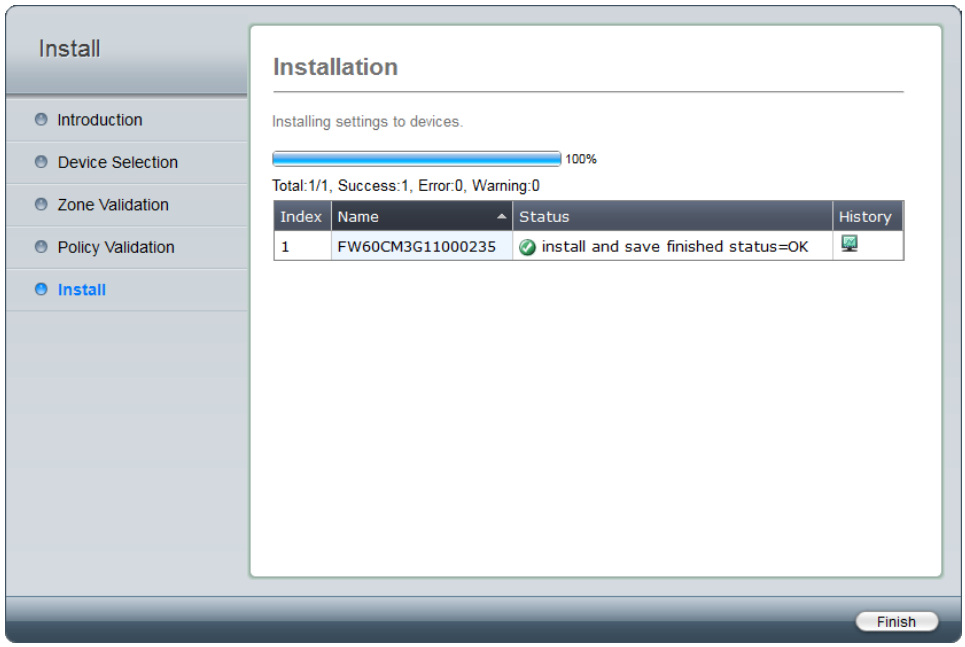
Figure 92: Policy package policy validation window



Installation

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

Figure 93: Policy package installation window



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

Figure 94: Device installation history

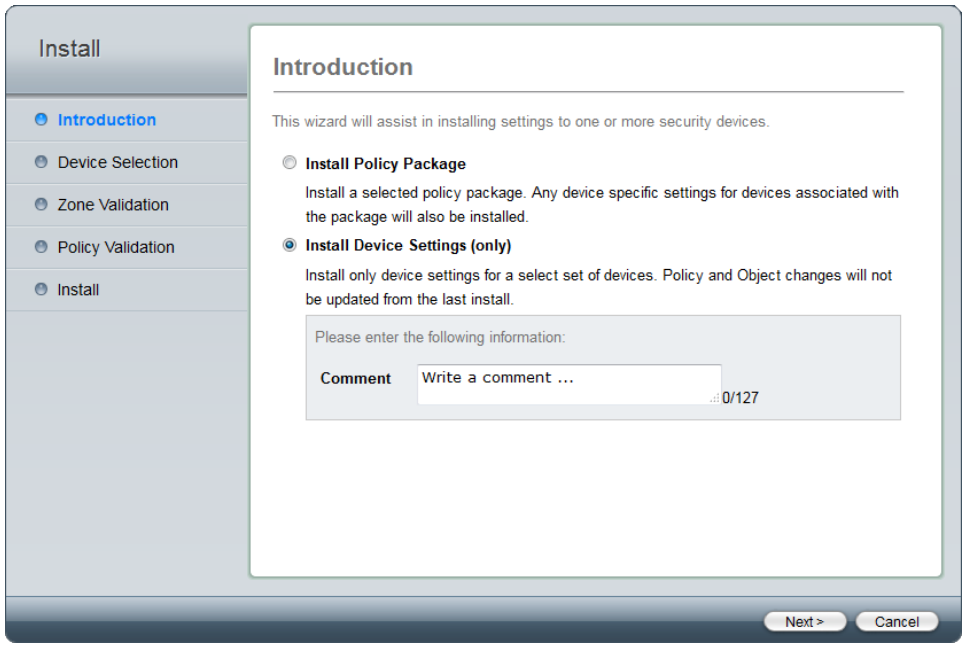
Task: 64, Record:1

Name	Percentage	Description
FW60CM3G11000235	0%	start to install dev(FW60CM3G11000235)
FW60CM3G11000235	15%	init state: start to get pre-checksum
FW60CM3G11000235	25%	get pre-checksum state: start get diff(chkout=1)
FW60CM3G11000235	35%	No cmds to be installed
FW60CM3G11000235	100%	install and save finished status=OK

Installing device settings

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

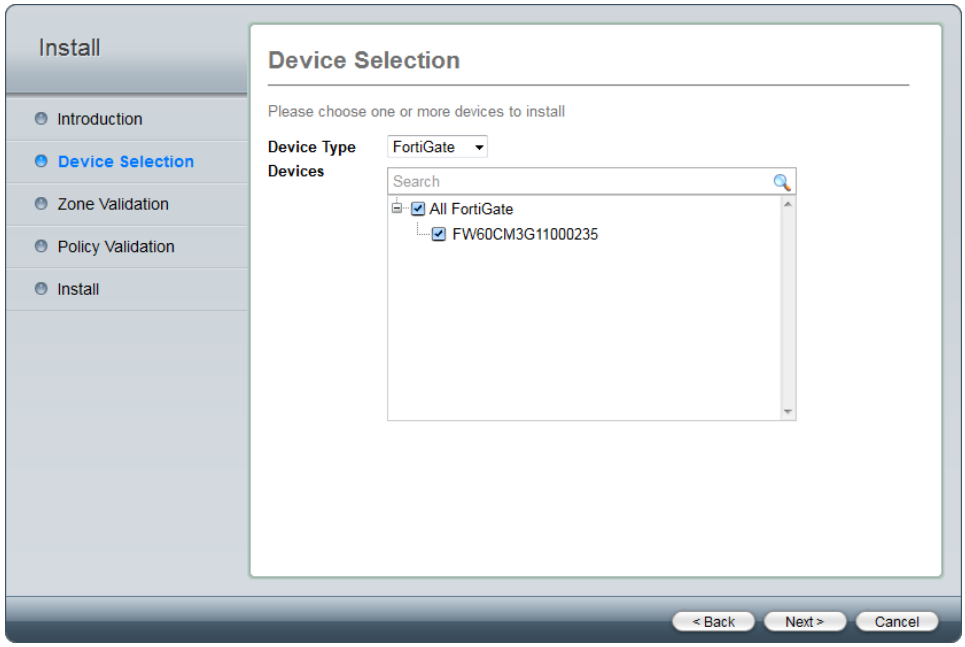
Figure 95: Install device settings only



Device selection

The device selection window allows you to choose the device type and then one or more devices of that type to install.

Figure 96: Device settings device selection window



Installation

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

Figure 97: Device settings successful installation window

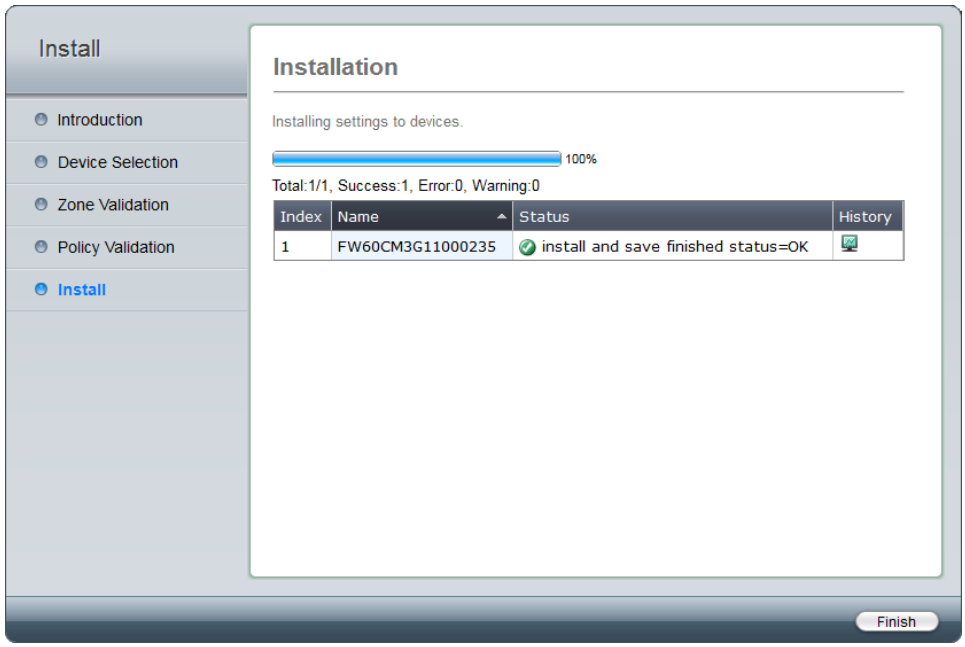
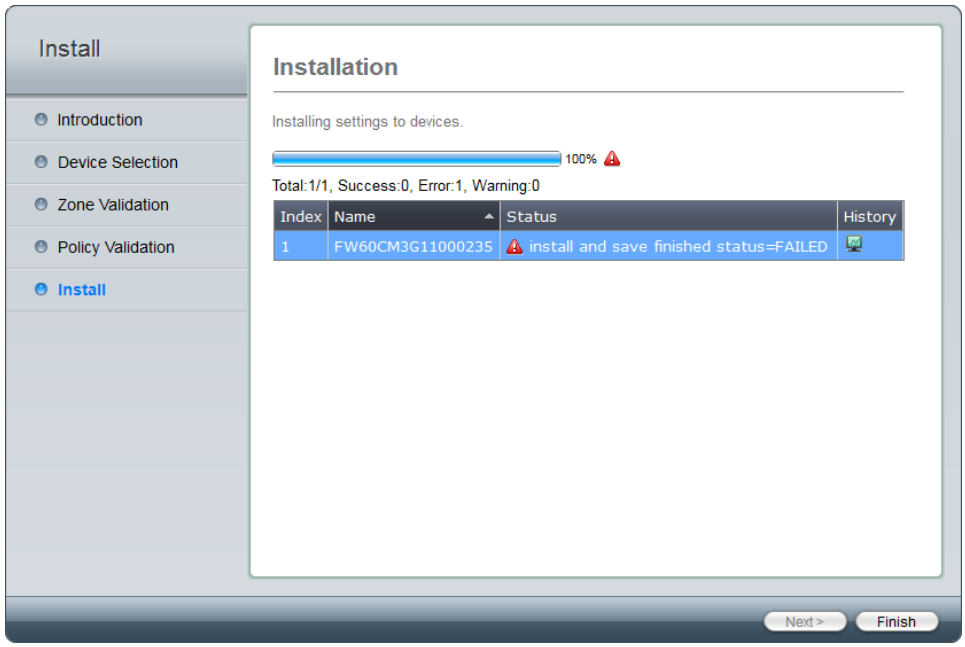


Figure 98: Device settings failed installation window



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

Figure 99: Device installation history

Task: 100, Record:1		
Name	Percentage	Description
FW60CM3G11000235	0%	start to install dev(FW60CM3G11000235)
FW60CM3G11000235	15%	init state: start to get pre-checksum
FW60CM3G11000235	25%	get pre-checksum state: start get diff(chkout=0)
FW60CM3G11000235	35%	script done state: start to FGFM install
FW60CM3G11000235	80%	fgfm install state: prepare to post-checksum
FW60CM3G11000235	90%	post-checksum state: start verification
FW60CM3G11000235	95%	verify state: install OK/verify FAIL
FW60CM3G11000235	10%	install and save start retry
FW60CM3G11000235	35%	script done state: start to FGFM install
FW60CM3G11000235	80%	fgfm install state: prepare to post-checksum
FW60CM3G11000235	90%	post-checksum state: start verification
FW60CM3G11000235	95%	verify state: install OK/verify FAIL
FW60CM3G11000235	100%	install and save finished status=FAILED

Overview of the add device wizard

The add device wizard allows you to provision a device prior to installation.

Use the Add Device Wizard to add a FortiGate device to an ADOM:

1. Log into the FortiManager Web-based Manager using an administrator account.
2. Select the Administrator Domain tab, go to All ADOMs and select the ADOM for which you want to add the device, from the drop down menu on the top navigation pane.
3. Select the *Device Manager* tab. To add a device, you can either select the Add Device icon on the top pane or right click in the body pane and select Add > Device on the right-click menu. This will launch the Add Device Wizard.
4. There are two options within the wizard. The Discover option and the Add Model Device. Select Discover and enable the Import Device checkbox to import the policies and objects associated with the device.
5. Enter the IP Address of the FortiGate device, the device User Name and Password, select Next. The wizard will go through the discovery phase and collects device information. Select Next to continue.
6. You have the option to change the device host name, description, add the device to an existing group, and enter device specific information including the Company/Organization name and address. Select Next to continue.
7. The import wizard will go through various phases to retrieve device information, configuration, and create the device for import. When the device has been successfully created, select Next to continue.
8. If the device has virtual domains (VDOMs), you will have the option to import any or all of the VDOMs. When importing a VDOM, the wizard will allow you to map zones or add default zone mapping to unused interfaces. The second stage of the wizard allows you to import the VDOM policy database, you can select to import any or all of the VDOM policies, select Next to continue.
9. The Zone Map phase allows you to map zones for each interface. Select Add mappings for all unused interfaces to automatically create zones for unused interfaces, select Next to continue.
10. The Policy phase allows you to import all or select specific policies and profile groups to import with the device. Select either Import All or specify policies and profile groups and select Next to continue.
11. The Object phase will search for available objects and display results. Select Next to proceed.
12. The Import phase will complete the import of the device into the FortiManager, based on your selections in the previous screens. Select Next to continue.

13. The Summary will provide you with details of the FortiGate device and notify you that the device has been successfully added to the FortiManager. You can select Download Import Report to save a .txt copy of the summary to your local hard drive for reference. Select Finish to close the Import Wizard.

FortiManager Cookbook video link

http://www.youtube.com/watch?v=XjLVTuYN_Gw&list=PL29F8DE57AA4CA091&index=1&feature=plpp_video

Device Management

Device manager overview

Use the *Device Manager* tab to configure the devices that you have added. For more information on adding devices or virtual domains, see “Managing devices” on page 141.

This section focuses on FortiGate configuration using the FortiManager system. There are some tasks that cannot be performed or are performed differently on a FortiGate unit using the FortiGate Web-based Manager.

Viewing device summaries

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

This section contains the following topics:

- Viewing managed devices
- Viewing a single device
- Using list filters

Viewing managed devices

In the navigation pane select the *Device Manager* tab and the device type — FortiGate, FortiCarrier, FortiSwitch, FortiMail — to display all units of the selected type that are managed by the FortiManager system. You can then select a single unit in the device tree to display a list of all of its managed devices on one screen.

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

Right-clicking in a device row opens the right-click menu. It allows you to select one of following options: *Add (Device or Virtual Domain), Edit, Delete, Refresh, Import Policy, Column Settings, or Clear Filter*. See “Managing devices” on page 141 for more information.

Figure 100: Device manager device list layout

Figure 101: Right click menu options

The options are available:I

Right Click Menu Options	
Add	Select to Add a new device or virtual domain.
Edit	Edit device information. See “Editing device information” on page 143. Editing the information for a device is not the same as editing the configuration settings. For information on modifying the configuration settings of a device, see “Configuring devices” on page 150.
Delete	Select the check box beside a device that you want to delete, then select *Delete* to remove the device. See “Deleting a device” on page 143.
Refresh	Refresh the connection between the selected devices and the FortiManager system. See “Refreshing a device” on page 144. This operation updates the device status and the FortiGate HA cluster member information.
Import	Select to import a local device. See “Importing and exporting devices” on page 145.
Export	Select to export the device list. See “Importing and exporting devices” on page 145.
Column Settings	Select to change column settings to control the information columns that are displayed for the list and to control the order in which they are displayed.
Clear Filter	Select to clear filter information.
Menu Bar Options	
Add Multiple	Select to add multiple new devices.
Import Device List	Select to import a device list from your local hard drive (HDD).
Export Device List	Select to export the device list to a text file. You can save the file to your local hard drive (HDD).
Device Manager Fields	
Device Name	The name of a device.

Config Status	The config status. When a conflict occurs, a red star surrounded by an orange circle will be displayed.
Connectivity	The status of the device and the time and date the status was last checked. A green arrow indicates the connection between a device and the FortiManager system is up. A red arrow indicates the connection is down.
Arrow	When displayed, select to expand device view to display the summary for the configured VDOMs. For more information, see "Configuring virtual domains (VDOMs)" on page 151.
Virtual Domain	If a device has VDOMs, a blue arrow appears beside it. Select the arrow to display the VDOM summary. Select the VDOM name to view or edit the VDOM configuration. For more information, see "Configuring virtual domains (VDOMs)" on page 151.
IP	Displays the IP address of the connected device.
Platform	Displays the device platform type, for example, FortiWiFi-30B.
FortiGuard Services	The status of antivirus, intrusion protection, web filtering, email filtering, and vulnerability scan licenses for the device.
Description	Displays the optional description of the connected device.

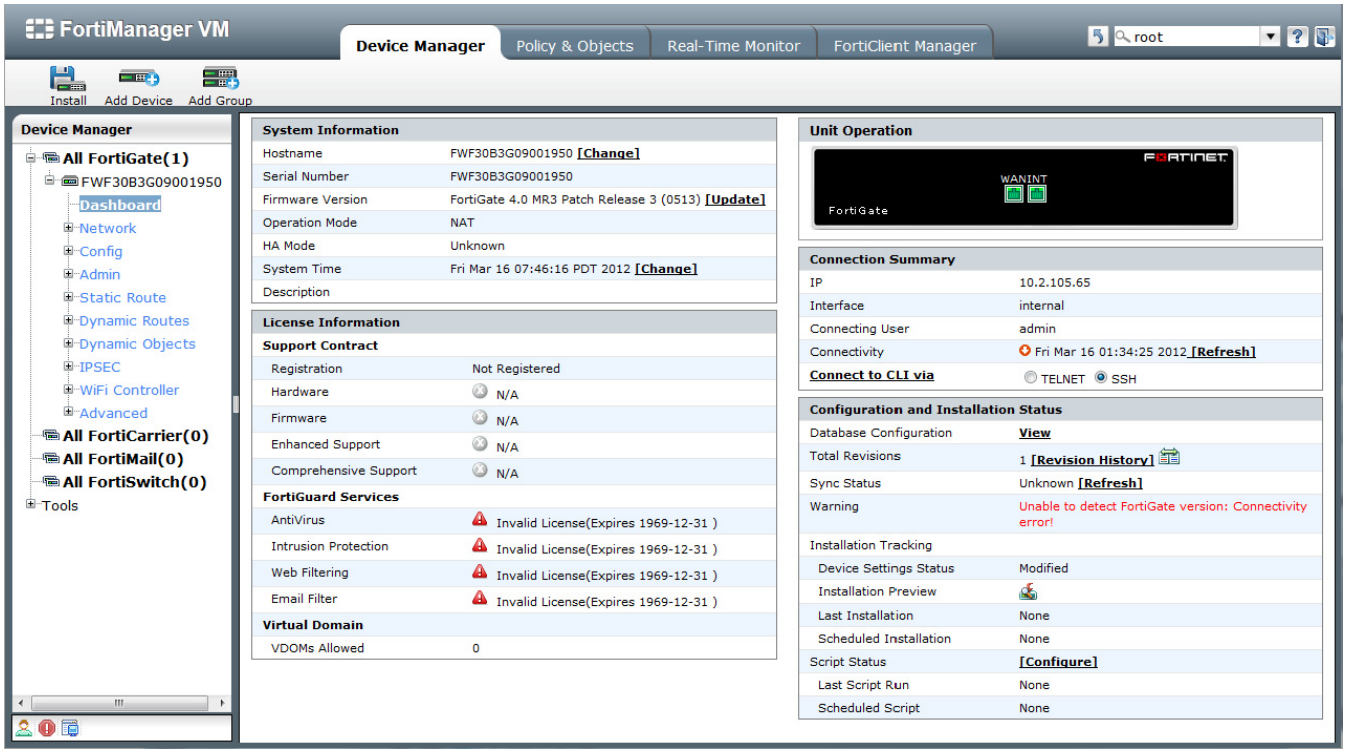
Viewing a single device

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

To view a device, in the navigation pane, select *Device Manager* > *All FortiGate*, and select a device in the content pane.

By default, the navigation pane will display the navigation options for that device — normally System, Router, Firewall, UTM, VPN, User, WAN Optimization, Endpoint Security, WiFi Controller, and Log & Report. For details about device fields, see the FortiGate documentation for the specific feature. The content pane displays the status information for the selected device.

Figure 102: Example FortiGate unit summary



The following information is available:

License Information	
Support Contract	The support contract information and the expiry date. The support contract includes the following: Registration, Hardware, Firmware, Support Level e.g. 8x5 & 24x7.
FortiGuard Services	The contract version, issue date and service status. FortiGuard Services includes the following: antivirus, Intrusion Protection, Web Filtering, and email filtering.
Virtual Domain	The number of virtual domains that the device supports.
System Information	
Hostname	The name of the device.
Serial Number	The device serial number.
Firmware Version	The device firmware version and build number.
Operation Mode	Operational mode of the FortiGate unit: NAT or Transparent.
HA Mode	Standalone indicates non-HA mode.
System Time	The device system time and date information.
Description	Descriptive information about the device.

Unit Operation	An illustration of the FortiGate unit's front panel showing the unit's Ethernet network interfaces. For more information, see the *FortiGate Administration Guide*.
Connection Summary	
IP	The IP address of the device.
Interface	The port used to connect to the FortiManager system.
Connecting User	The user name for logging in to the device.
Connectivity	The device connectivity status and the time it was last checked. A green arrow means that the connection between the device and the FortiManager system is up; a red arrow means that the connection is down. Select *Check Now* to test the connection between the device and the FortiManager system.
Connect to CLI via	Select the method by which the you connect to the device CLI, either SSH or TELNET.
Configuration and Installation Status	
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.
Diff with Saved Revisions	Select *Diff* icon to show only the changes or differences between the saved configuration revision and another revision. For more information, see "Comparing different configuration files" on page 189.
Configuration Change Status	One of the following: *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. For more information, see "Configuring devices" on page 150.
Installation Status	One of the following: *Synchronized*: The latest revision is confirmed as running on the device. *Out_of_sync*: The configuration file on the device is not synchronized with the FortiManager system. *Unknown*: The FortiManager system is unable to detect which revision (in revision history) is currently running on the device. Select *Refresh* to update the Installation Status.
Installation preview	Select icon to display a set of commands that will be used in an actual device configuration installation in a new window.

Warning	One of the following: *None*: No warning. *Unknown configuration version running on FortiGate: FortiGate configuration has been changed!*: The FortiManager system cannot detect which revision (in *Revision History*) is currently running on the device. *Unable to detect the FortiGate version*: Connectivity error! *Aborted*: The FortiManager system cannot access the device.
Installation Tracking	One of the following: *Last Installation*: The FortiManager system sent a configuration to the device at the time and date listed. *Scheduled Installation*: A new configuration will be installed on the device at the date and time indicated.
Out-of-Sync	This option appears when the version of the configuration saved on the FortiManager repository is different from the one on the device. You can retrieve the latest configuration.

Using list filters

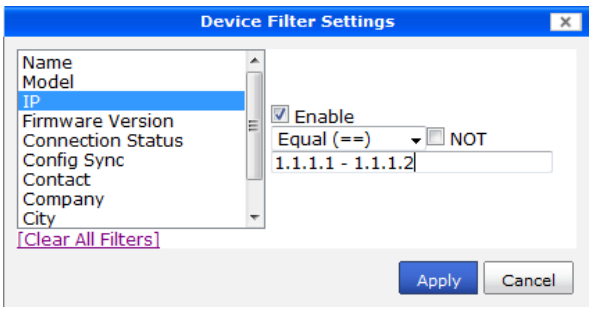
You can enable filters to control the information that is displayed by the device list. Filters are useful for reducing the number of entries that are displayed on a list so that you can focus on the information that is important to you.

You add filters to a device list by going to *Device Manager* in the navigation pane and selecting a device group, then the *Filter* button in the content pane to display the *Device Filter Settings* window. From this window, you can select any column name to filter, and configure the filter for that column. You can also add filters for one or more columns at a time.

Filters for columns that contain numbers

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

Figure 103: Device filter settings dialog box

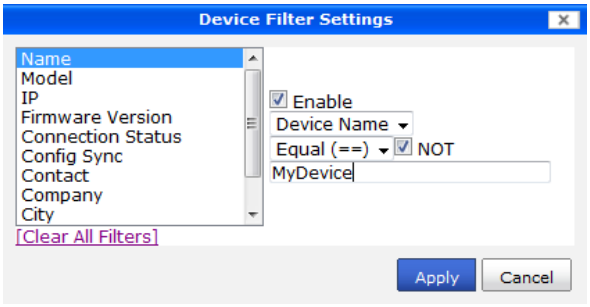


Filters for columns containing text strings

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

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

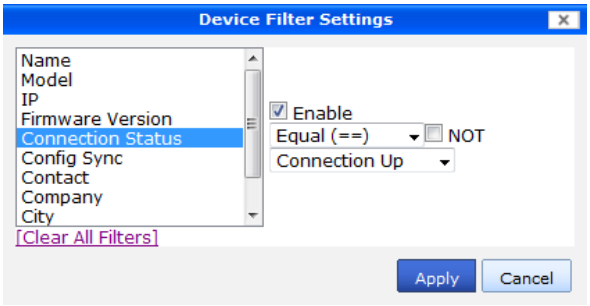
Figure 104: Device filter settings dialog box



Filters for columns that can contain only specific items

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

Figure 105: Device filter settings dialog box



Managing devices

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

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

This section includes the following topics:

- Adding a device
- Replacing a managed device
- Deleting a device

- Editing device information
- Refreshing a device
- Importing and exporting devices
- Setting unregistered device options

Adding a device

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

For an existing device, use the *Add Device* function and follow the steps in the add device wizard. Adding an existing device will not result in an immediate connection to the device. Device connection happens only when you successfully resynchronize the device.

Adding an operating FortiGate HA cluster to the *Device Manager* is similar to adding a standalone device. For more information, see "Configuring High Availability" on page 76.

To add a device:

1. From the main menu bar, select *Add Device*.
2. Follow the steps in the add device wizard to add the device. See "Adding a Device" on page 123.

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 re-install a device that has a *Retrieve* button under the *Revision History* tab. For more information, see "To re-install the configuration:" on page 142.

To change the serial number:

1. Configure the new device's IP address, gateway, admin password, and SSH/HTTPS access, and connect it to the FortiManager system. For more information, consult your device's documentation.
2. Record the host name of the old device.
3. Use the following CLI command to replace the serial number of the old device with that of the new device:

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

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

To re-install the configuration:

1. In the *Device Manager* tab, select *FortiGate, FortiSwitch, FortiCarrier, or FortiMail* in the navigation pane.
2. In the content pane, select a device's name.
3. Select *Revision History* for that device in the *navigation pane.*

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

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

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

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

   For more information, see "Downloading and importing a configuration file" on page 189.

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

Deleting a device

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

To delete a device:

1. In the *navigation pane*, select *Device Manager* and the type of device.
2. In the content pane, select the check box for the device or devices to be deleted and select *Delete*, or right-click on the device's row and select *Delete* from the right-click menu.

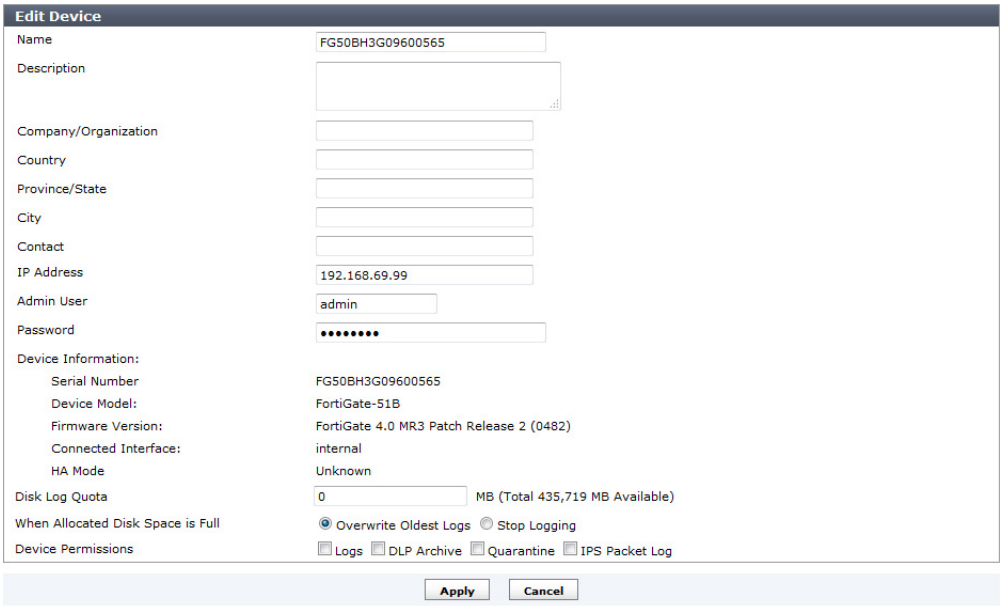
Editing device information

You can edit the *Name*, *Description*, *IP address*, *Admin User*, and *Password* on single devices.

To edit information for a single device:

1. In the *navigation pane*, select the device type that you want to edit.
2. Select a device from the device list then select the *Edit* icon, or right-click on the device row and select *Edit* from the right-click menu.

Figure 106: Edit device



3. Configure the following settings:

Name	The name of the device.
Description	Descriptive information about the device.
Company /Organization	Enter the company information.
Country	Enter country information.
Province/State	Enter province/state information.
City	Enter city information.
Contact	Enter contact information.
IP Address	The IP address of the device.
Admin User	The admin user username.
Password	The admin user password
Device Information	Information about the device, including serial number, device model, firmware version, connected interface, and HA mode.
Disk Log Quota	The amount of space that the disk log is allowed to use, in MB.
When Allocated Disk Space is Full	The action for the system to take when the disk log quota is filled.
Device Permissions	The device's permissions.

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

See also

- Importing and exporting devices

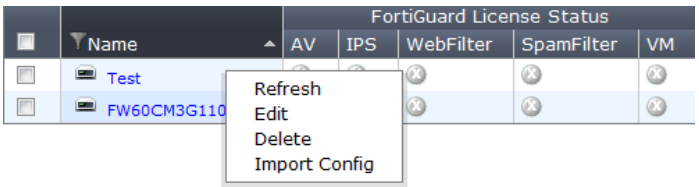
Refreshing a device

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 navigation pane, select the *Device Manager* tab and then select a device group.
2. Select a device from the device list then select the *Refresh* icon, or right-click on the device row and select *Refresh* from the right-click menu.

Figure 107: Device manager right-click menu



3. A warning message will ask you if you are sure you want to update the selected device, select *OK* to refresh the device.

Importing policies to a device

Importing policies to a device is done using a shortened version of the Add Device wizard.

To import policies to a device:

1. In the navigation pane, select the *Device Manager* tab and then select a device group.
2. Select a device from the device list then right-click on the device row and select *Import Policy* from the right-click menu.
3. The Import Device Wizard opens at the Zone Map window. See "Importing a device" on page 119 for more information.

Importing and exporting devices

You can import or export large numbers of devices, ADOMs, device VDOMs, and device groups in one operation, using a specially formatted text file.

There are two ways to create the text file:

- **Use a backup file**. You can use the device *Export* feature to save a list of devices in a text file as a backup and import the file later.

  When you select *Export* in the Main Menu Bar, it does not actually remove the devices from the FortiManager system. A list of devices is saved to the location you specified. It can be used as a backup file and imported later.The exported list contains the full device details.
- **Create the file manually**. For more information, see "Example text files" on page 148.

To bulk import devices:

1. In the navigation pane, select the *Device Manager* tab and then select a device group.
2. In the content pane, select *Import*.
3. Select *Browse* and locate and specify the device list text file.
4. Select *Submit*.

To bulk export devices:

1. In the navigation pane, select *Device Manager* and type of device.
2. In the content pane, select *Export*.
3. Save the file.

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=7
```

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.

Device file format

Devices are specified by the following device lines:

```
device_list_ver=7
device|ip|name|platform|admin|passwd|adom|desc|discover|reload|fwver
     |mr|patch|build|branch_pt|interim|sn|has_hd|
```

The fields after “reload” are optional, and only need to be provided if discover is set to 0.

The list in the text file should contain the following fields:

Field Name	Blank Allowed	Description
ip	No	Device IP address.
platform	No	The device type. For example, FortiGate, or the full platform name: FortiWiFi-60B.
user	No	Admin username.
passwd	Yes	Admin password.
adom	Yes	The ADOM into which this device should be imported. If this field is left blank, the device is imported into the current ADOM.
desc	Yes	Device description.
discover	No	Enter 1 to automatically discover device, 0 otherwise.
reload	No	Enter 1 to reload the device configuration after importing it, 0 otherwise.
fwver	No	Firmware version.
mr	No	Major Revision (MR) designation of the device. For example, GA, MR1, MR2.
sn	No	Device serial number.
has_ha	No	Enter 1 if the device has a hard disk, 0 if not.

Following the device line, there may be one or more “+meta” lines specifying metadata for the device (For more information, see “Metadata file format” on page 148), or one or more “+vdom” lines specifying device VDOMs.

VDOMs are specified by the following lines:

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

Field Name	Blank Allowed	Description
devname	No	Name of the device.

vdom	Yes	The VDOM of the device that belongs to this group. If this field is left empty, the VDOM refers to the root VDOM.
groupname	No	The name of the subgroup that belongs to this group. Note that only 2 levels of group nestings are permitted in FortiManager v4.0.

ADOM file format

ADOMs are specified by the following ADOM lines:

```
device_list_ver=7
adom|name|mode|enable|
```

One or more "+meta" lines may follow a ADOM line to specify the values of metadata associated with that ADOM. See "Metadata file format" on page 148.

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

Group file format

Device group are specified as follows:

```
device_list_ver=7
group|name|desc|adom|
```

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

One or more "+meta" lines describing metadata values for the group, or one or more lines describing group members and subgroups, may follow the group line. See see "Metadata file format" on page 148.

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

Field Name	Blank Allowed	Description
devname	No	Name of the device.

vdom	Yes	The VDOM of the device that belongs to this group. If this field is left empty, the VDOM refers to the root VDOM.
groupname	No	The name of the subgroup that belongs to this group. Only two levels of group nestings are permitted in FortiManager v4.0.

Metadata file format

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

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

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

String transliterations

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

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

Example text files

Here are three examples of what a text file might look like.

Example 1: Device

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

device|10.0.0.74|top|FortiGate|admin||root|My description.|1|1|
+meta|bogosity|10|
+vdom|vdom01|root|
```

```
+vdom|vdom02|root|
+vdom|vdom03|root|
+vdom|vdom04|root|

device|10.0.0.75|bottom|FortiGate-400A|admin|password|adom01|Your
     description.|0|1|4.00|MR3|FG400A2905550018|0|
+meta|bogosity|12|
+vdom|vdom01|adom01|
```

Example 2: ADOM

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

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

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

Example 3: Device group

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

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

group|group02|Another description.|root|
+meta|supervisor|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 / discovery fails, there must be appropriate event logs generated so you can trace what occurred.

Setting unregistered device options

To choose how FortiManager system handles unregistered devices, from the navigation pane, select *Device Manager* > *Unregistered Device* > *Unregistered Devices Options*.

Add unregistered devices to device table, but ignore service requests	Unregistered devices are automatically added to the *Unregistered Devices* list, but cannot receive FortiGuard updates.
Add unregistered devices to device table, and allow FortiGuard service and central management service	Unregistered devices are automatically added to the *Unregistered Devices* list and subscribers to the FortiGuard service can receive updates.
Apply	Select to save the setting.

Configuring devices

You can configure the FortiGate units in two ways:

- By selecting a single device from the *Device Manager*, you can configure the settings of this device.
- By selecting a virtual domain (VDOM) from the *Device Manager*, you can configure settings for that virtual domain.

This section contains the following topics:

- Configuring a device
- Configuring virtual domains (VDOMs)

Configuring a device

Configuring a FortiGate unit using the *Device Manager* tab is very similar to configuring FortiGate units using the FortiGate Web-based Manager. You can also save the configuration changes to the configuration repository and install them to other FortiGate unit(s) at the same time. For more information, see "Managing configuration revision history" on page 187.

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

To configure a FortiGate unit:

1. In the *Device Manager* tab, select the unit you want to configure.
2. Select an option (such as System, Router, Firewall, UTM, VPN, User, Endpoint Control, or Log & Report) for that unit in the *Device Manager* tab.
3. Configure the unit as required.

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

You can rename and reapply firewall objects such as address, address group, service, schedule, VIP, load balance, protection profile, and traffic shaping after they are created and applied to a firewall policy. When you do so, the FortiManager system will:

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

Firewall policy reordering on first installation

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

This behavior is normal for the following reasons:

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

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

This behavior would only be seen:

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

Configuring virtual domains (VDOMs)

Virtual domains (VDOMs) enable you to partition and use your FortiGate unit as if it were multiple units. For more information see the *FortiGate Administration Guide* or the *VLAN and VDOM Guide*.

To view the VDOM list, in the FortiGate menu of a device, select *System* > *Virtual Domain* > *Virtual Domain*.

Delete	Select to remove this virtual domain. This function applies to all virtual domains except the root.
Create New	Select to create a new virtual domain.
Management Virtual Domain	Select the management VDOM and click Apply.
Name	The name of the virtual domain and if it is the management VDOM.

Virtual Domain	Virtual domain type.
IP/Netmask	The IP address and mask. Normally used only for Transparent mode.
Type	Either VDOM Link or Physical.
Access	HTTP, HTTPS, SSH, PING, SNMP, and/or TELNET.
Resource Limit	Select to configure the resource limit profile for this VDOM. For more information, see "Configuring VDOM resource limits" on page 154 and "Configuring VDOM global resources" on page 154.

Creating and editing virtual domains

Creating and editing virtual domains in the FortiManager system is very similar to creating and editing VDOMs using the FortiGate Web-based Manager.

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

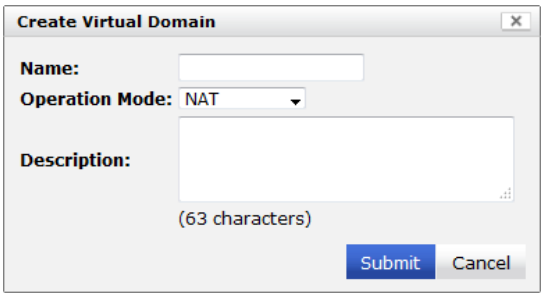
To enable virtual domains:

1. In the *Device Manager* tab, select the unit you want to configure.
2. In the FortiGate menu of a device, select *System* > *Dashboard* > *Status*.
3. In the *System Information* area, click the *Enable* link in the *Virtual Domain* field.

To create a virtual domain:

1. In the *Device Manager* tab, select the unit you want to configure.
2. In the FortiGate menu, select *System* > *Virtual Domain* > *Virtual Domain*.
3. Click *Create New*.

Figure 108: Create new virtual domain



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

   The new VDOM will appear in the list.

Configuring 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. This feature is only available through the FortiGate CLI. For more information on inter-VDOM routing see the VDOM Admin chapters of the FortiGate CLI Reference.

Before configuring inter-VDOM routing:

- you must have at least two virtual domains configured.
- the virtual domains must all be in NAT/route mode.
- each virtual domain to be linked must have at least one interface or subinterface assigned to it.

To create an inter-VDOM link:

1. In the *Device Tree*, select a virtual domain.
2. Select the *Configuration* tab.
3. On the *Device Summary* page, select the blue arrow to expand *Configure Inter-VDOM Routing*.

   If there is no blue arrow, there is only one virtual domain. You must create at least one more virtual domain before continuing.

VDOM	Name of the virtual domain to link the current virtual domain with.
VDOM Link Name	The name of the link that will inter-connect the current to the selected virtual domain.
IP Addressing	
Testing	IP address and netmask of the current virtual domain, the starting point of the link between the two virtual domains.
peer vdom	IP address and netmask of the non-current virtual domain, the end point being linked. For example if the VDOM selected is vdom2, that is the peer vdom.
Traffic log	Select to log the traffic on this interface.

4. Select the check box next to the VDOM to be linked to the current VDOM (the one selected in step 1).
5. Enter a name for the inter-VDOM link. Both virtual interfaces will use this name. For example, if the link is “my_vlink”, the virtual interfaces created will be “my_vlink0” and “my_vlink1”.
6. Enter the IP address and netmask for the virtual interface of this link on the current VDOM and the peer VDOM. For example, if the current VDOM is vdom1, root could be the peer VDOM.

   Once the inter-VDOM link is created, these IP addresses cannot be changed without deleting the link.
7. Select *Traffic Log* to log the traffic on this inter-VDOM link.
8. Select *Apply* to save your settings.

You can repeat these steps to create other inter-VDOM links if you have more than two VDOMs.

To remove an inter-VDOM link, clear the check box next to it and select Apply. Both ends of the link will be removed.

See also

- Configuring devices

Configuring VDOM resource limits

A VDOM's resource limit defines how much resources a VDOM can consume. You can set a VDOM's maximum and guaranteed limits for each resource. You can also view the current usage of the resources by the VDOM.

A VDOM's maximum limit for a resource cannot be greater than the global maximum limit set for this resource. This value is not guaranteed if you have more than one VDOM with each one having a maximum limit value and all are running at the same time.

A VDOM's guaranteed resource limit is the actual amount of resource a VDOM can use regardless of the number of VDOMs running at the same time. Although each VDOM can have its own guaranteed limit, the sum of guaranteed resource limits for all VDOMs must be less than or equal to the global maximum resource limit.

For more information, see "Configuring VDOM global resources" on page 154.

To configure a VDOM's resource limits:

1. In the *Device Manager* tab, select the unit you want to configure.
2. In the FortiGate menu, select *System* > *Virtual Domain* > *Virtual Domain*.
3. Click the *Resource Limit* icon of a VDOM.
4. For each resource:
   - enter the maximum value allowed for this resource. If you enter a wrong value, a warning appears with the correct value range.
   - enter the value allocated for this resource. This value must be lower than or equal to the maximum value.
5. Click *OK*.

Configuring VDOM global resources

You can set a maximum limit for each resource that each VDOM in a device can consume. Each VDOM's maximum limit cannot exceed the global maximum limit set for the same resource. This is a good way to allocate network resources.

To configure VDOM global resources:

1. In the *Device Manager*, select the unit you want to configure.
2. In the FortiGate menu, select *System* > *Virtual Domain* > *Global Resources.*

Resource	The network resources that the VDOMs can use.
Configured Maximum	The maximum resource limit for all VDOMs set by the user. For more information, see "Edit icon" on page 154.
Default Maximum	The default maximum resource limit for all VDOMs.
Current Usage	The total consumption of the resource by all VDOMs.
Edit icon	Select to set a maximum resource limit for all VDOMs.
Reset to default value	Select to set the configured maximum limit to the default maximum limit.

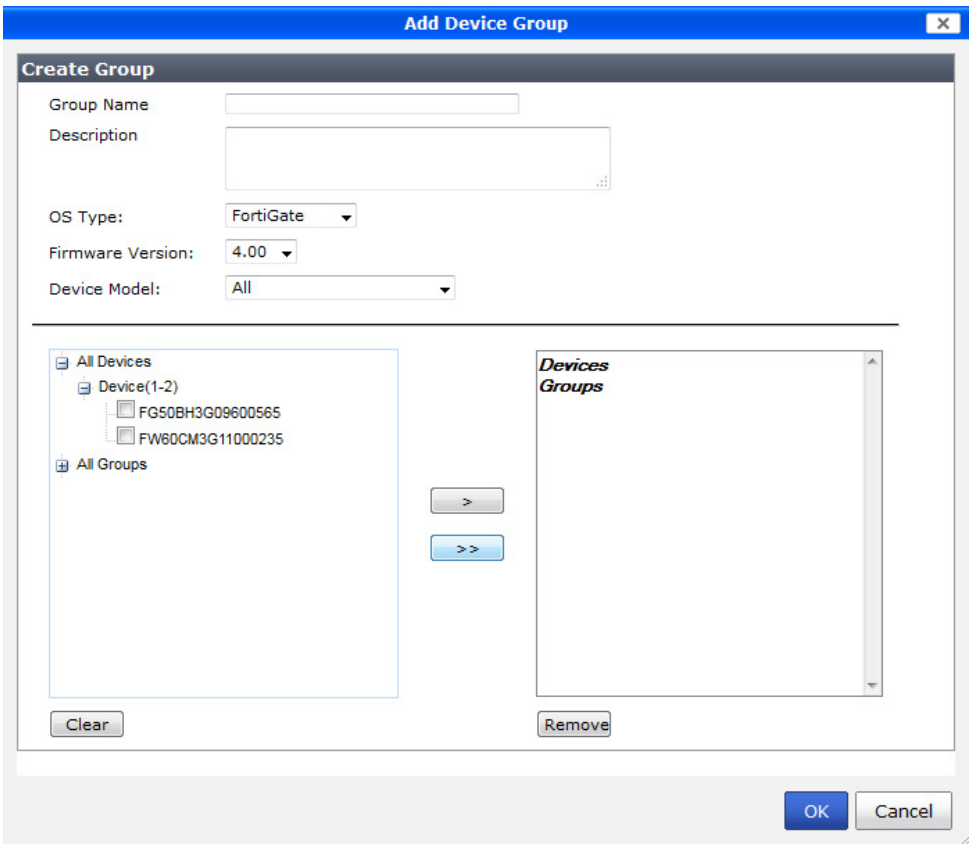
Working with device groups

Adding a device group

To add a group

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

Figure 109: Adding a group



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

Group Name	Enter a unique name for the group (maximum 32 characters). The name cannot be the same as the name of another device or device group and may only contain numbers, letters, and the special characters '-' and '_'.
Description	Enter a description for the group. The description can be used to provide more information about the group, such as its location.
OS Type	Select an OS type, such as FortiGate or FortiMail, from the drop-down list.
Firmware Version	Select a firmware version for the group. All members of the group must run this firmware version.
Device Model	Select a device model.
Add icon	Move the selected device or group from the device list to the group member list.

Replace icon	Replace one or more devices in the group member list with selected ones in the device list.
Clear	Clear the selections in the device list.
Remove	Clear the selected devices in the group member list.

3. Select *OK* to add the group.

Deleting a device group

You can delete groups from the FortiManager system.

To delete a group:

1. In the *navigation pane*, select *Device Manager* > Group
2. In the content pane, select the check box for the group or groups to be deleted.
3. Select *Delete*.

Editing device group information

You can edit the all the details of a single group.

To edit information for a single group:

1. In the *navigation pane*, select *Devices* > *Group*.
2. In the content pane, either select the check box for the group to be edited and select the *Edit* icon, or click on the group to be edited and select *Edit Group* from the group summary page.
3. Make the appropriate changes and select *Apply*. For more information, see "Adding a device group" on page 155.

Viewing the device group summary

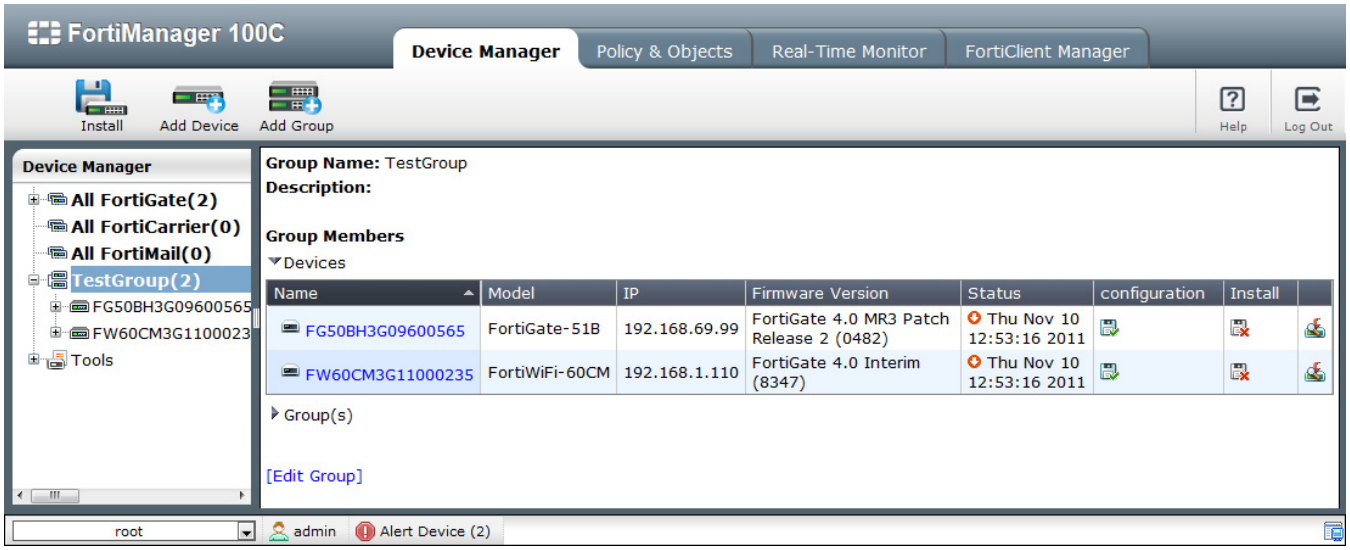
The device group summary shows the group name and description, and provides a list of all of the devices and groups within the group.

To view the device group summary:

1. In the *navigation pane*, select *Devices* > *Group*.
2. In the content pane, click on the name of the group to be viewed.

   The device group summary for that group opens.

Figure 110: Device group summary screen



3. Selecting the name of a device or group will open that device's or group's summary screen.
4. Selecting the *Edit Group* will open the Edit Group dialog box; see "Editing device group information" on page 156.

Managing FortiGate chassis devices

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

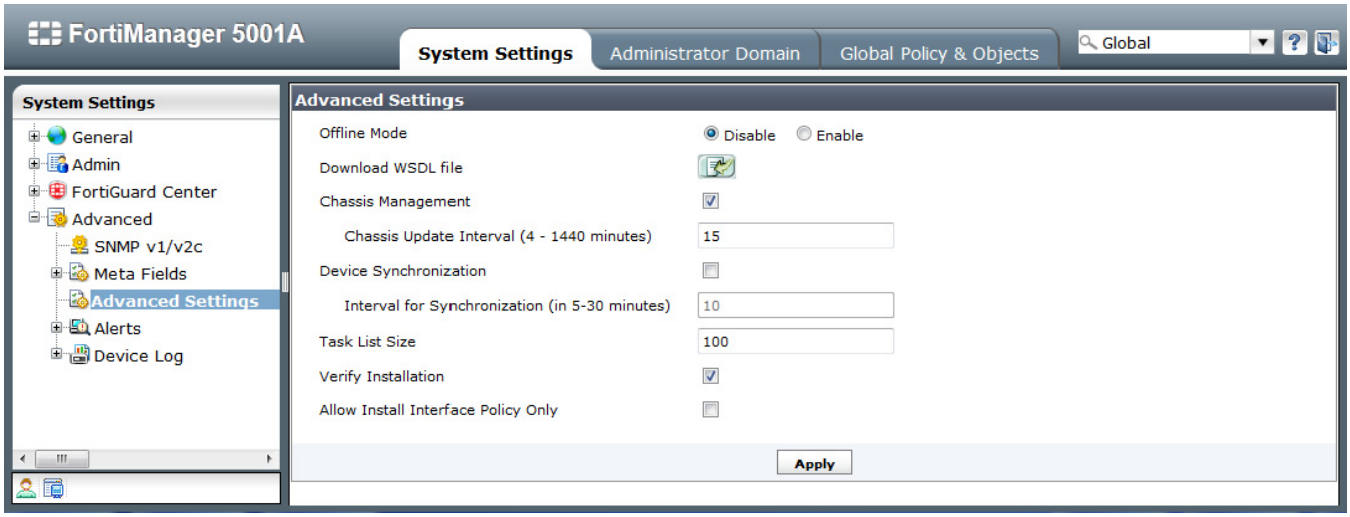
FMG-VM-1000-UG and FMG-5000UG support shelf manager for chassis management

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

To enable chassis management:

1. In the *System Settings* tab, go to *System Settings* > *Advanced* > *Advanced Settings*
2. Under *Advanced Settings*, select *Chassis Management*
3. Set the Chassis Update Interval, value range from 4 to 1440 minutes

Figure 111: Enable chassis management



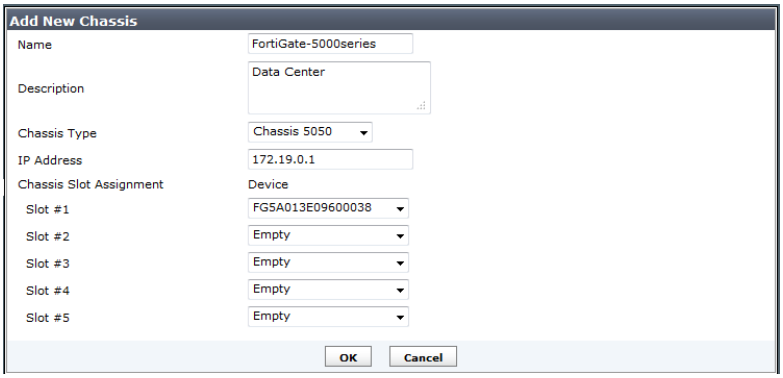
To view the chassis list, go to *Device Manager* > *All Chassis*.

Add Chassis	Select to add a new chassis. For more information, see "To add a chassis:" on page 158.
Delete	Select the check box beside a chassis that you want to delete, then select *Delete* to remove it.
Chassis detail (button)	Select to display the FortiGate-5000 series blades contained in the chassis slots. For more information about the FortiGate blades list, see "Viewing device summaries" on page 135.
Name	Select the name of the chassis to display the blades in that chassis. See "Viewing the status of the FortiGate blades" on page 160.
Model	The model of a chassis.
IP	The IP address of the Shelf Manager running on the chassis.
Edit icon	Edit chassis information and assign FortiGate-5000 series blades to the slots. For information, see "To edit a chassis and assign FortiGate-5000 series blade to the slots:" on page 159.
Update icon	Select to refresh the connection between a Shelf Manager and the FortiManager system.

To add a chassis:

1. In the navigation pane, go to *Device Manager* > *All Chassis*
2. In the content pane, select *Add Chassis*

Figure 112: Add new chassis



3. Configure the following settings:

Name	Enter a unique name for the chassis.
Description	Optionally, enter any comments or notes about this chassis.
Chassis Type	Select the chassis type: Chassis 5050, 5060, 5140 or 5140B.
IP Address	Enter the IP address of the Shelf Manager running on the chassis.
Chassis Slot Assignment	You cannot assign FortiGate-5000 series blades to the slot until after the chassis has been added. For information on assigning slots, see "To edit a chassis and assign FortiGate-5000 series blade to the slots:" on page 159.

4. Select *OK*.

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

1. In the navigation pane, go to *Device Manager* > *All Chassis.*
2. In the content pane, select the *Edit* icon of the chassis to edit.
3. Modify the fields except *Chassis Type* as required.
4. For *Chassis Slot Assignment*, from the drop-down list of a slot, select a FortiGate-5000 series blade to assign it to the slot. You can select a FortiGate, FortiCarrier, or FortiSwitch unit.

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

5. Select *OK*.

Viewing chassis dashboard

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

Viewing the status of the FortiGate blades

In the navigation pane, go to *Device Manager* > *All Chassis* and in the content pane, select the name of a chassis in the list. Optionally you can select Blade status from the navigation pane when the Chassis has been selected.

Refresh	Select to update the current page. If there are no entries, Refresh is not displayed.
Slot #	The slot number in the chassis. The FortiGate-5050 chassis contains five slots numbered 1 to 5. The FortiGate-5060 chassis contains six slots numbered 1 to 6. The FortiGate-5140 and -5140B chassis contains fourteen slots numbered 1 to 14.
Extension Card	If there is an extension card installed in the blade, this column displays an arrow you can select to expand the display. The expanded display shows details about the extension card as well as the blade.
Slot Info	Indicates whether the slot contains a node card (for example, a FortiGate-5001SX blade) or a switch card (for example, a FortiSwitch-5003 blade) or is empty.
State	Indicates whether the card in the slot is installed or running, or if the slot is empty.
Temperature Sensors	Indicates if the temperature sensors for the blade in each slot are detecting a temperature within an acceptable range. *OK* indicates that all monitored temperatures are within acceptable ranges. *Critical* indicates that a monitored temperature is too high (usually about 75°C or higher) or too low (below 10°C).
Current Sensors	Indicates if the current sensors for the blade in each slot are detecting a current within an acceptable range. *OK* indicates that all monitored currents are within acceptable ranges. *Critical* indicates that a monitored current is too high or too low.
Voltage Sensors	Indicates if the voltage sensors for the blade in each slot are detecting a voltage within an acceptable range. *OK* indicates that all monitored voltages are within acceptable ranges. *Critical* indicates that a monitored voltage is too high or too low.
Power Used	Indicates the amount of power being consumed by each blade in the slot.
Action	Select *Activate* to turn the state of a blade from *Installed* into *Running*. Select *Deactivate* to turn the state of a blade from *Running* into *Installed*.
Edit icon	Select to view the detailed information on the voltage and temperature of a slot, including sensors, status, and state. You can also edit some voltage and temperature values. For more information, see “To edit voltage and temperature values:” on page 161.
Browse icon	Select to update the slot.

To edit voltage and temperature values:

1. Go to *Device Manager* > *All Chassis* and in the content pane select the name of a chassis in the list.
2. In the navigation pane, select the *Blades* item.
3. Select the *Edit* icon of a slot.

   The detailed information on the voltage and temperature of the slot including sensors, status, and state displays.
4. Select the *Edit* icon of a voltage or temperature sensor.

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

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

Viewing the status of the power entry modules

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

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

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

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

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

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

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

Viewing shelf manager status

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

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

Viewing shelf alarm panel (SAP) status

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

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

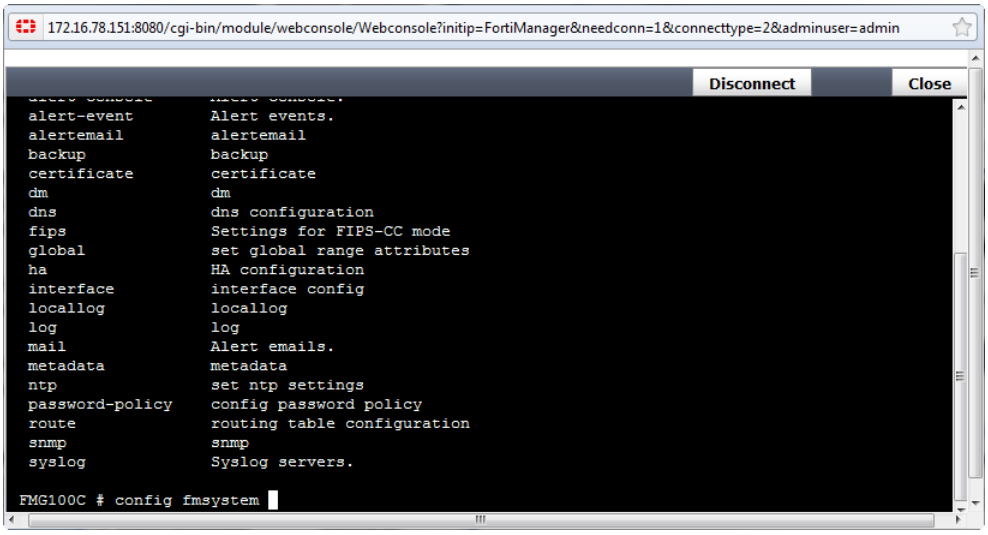
Presence	Indicates if the SAP is present or absent.
Telco Alarm	Telco form-c relay connections for minor, major and critical power faults provided by the external dry relay Telco alarm interface (48VDC).
Air Filter	Indicates if the air filter is present or absent.
Model	The SAP model.
State	The operation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

Using the CLI console for managed devices

You can access the CLI commands of the managed devices through the CLI Console on the System Settings Dashboard. To use the CLI, you connect via Telnet or SSH.

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

Figure 113:CLI console



The following options are available

Connect | Disconnect	Connect to the device you select, or terminate the connection.
Close	Exit the CLI console.

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

Policies and Objects

The *Policies and Objects* tab enables you to manage and configure the devices and clients that are managed by the FortiManager unit. This includes the basic network settings to connect the device to the corporate network, antivirus definitions, attack signatures, access rules, and managing and updating firmware for the devices.

If the administrator account you logged on with does not have the appropriate privileges, you will not be able to edit or delete settings, or apply any changes. Instead you are limited to browsing. To modify these settings, see “Configuring administrator profiles” on page 85.

This section describes the following topics:

- About policies
- Policy workflow
- Managing policy packages
- About objects and dynamic objects
- Managing objects and dynamic objects

About policies

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

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

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

Figure 114: Management module

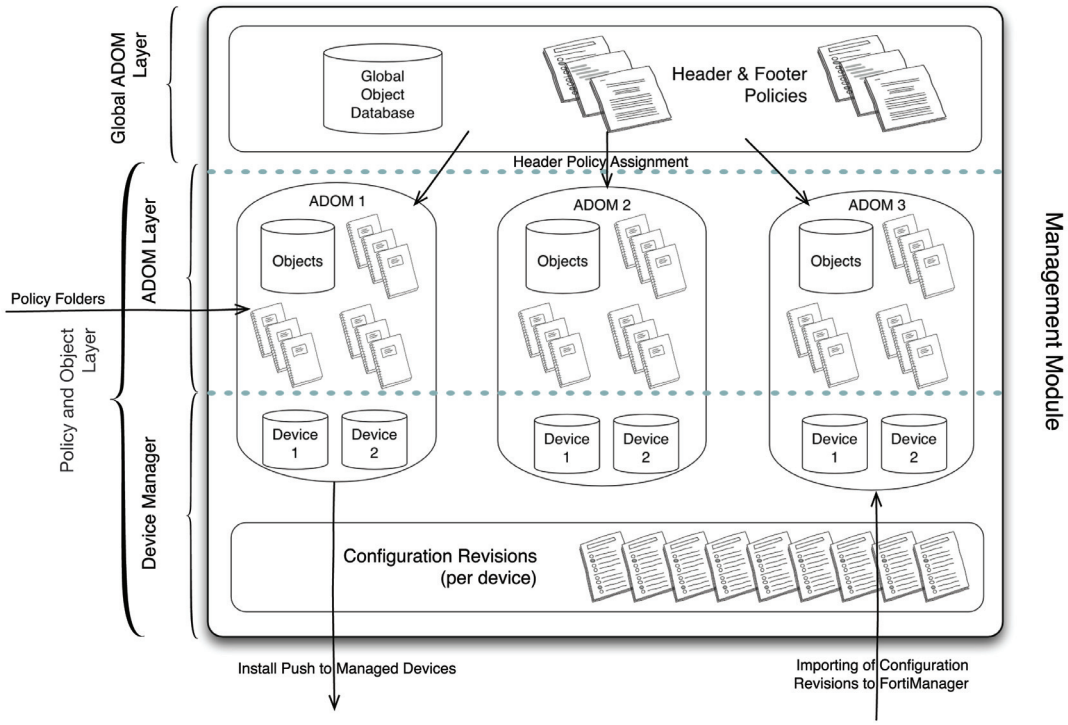
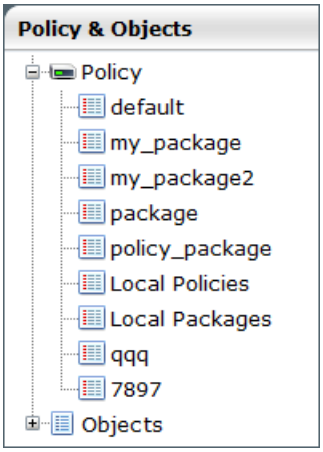


Figure 115: Policy window



Policy theory

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

Security policies are instructions units used 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 by using virtual IPs or IP pools to translate source and destination IP addresses and port numbers.

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

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

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

- Source Interface/Zone
- Source Address
- Destination Interface/Zone
- Destination Address
- Schedule and time of the session's initiation
- Service and the packet's port numbers.

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

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

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

Create security policies based on traffic flow. For example, 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 view log messages as to where the source and destination of the packets can seem backwards.

Policy workflow

An administrator will typically carry out 2 main functions with their devices or clients 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.

To provision a new device:

1. In the *Device Manager*, create a new VDOM or add a new device using “Add Device”.
2. Using *Device Manager*, configure any Dynamic Objects you wish to assign to the new VDOM or device.
3. Determine how a policy will be defined for the new device: does the new device or VDOM have a new policy package unique to itself or will use a package that is implemented elsewhere?
4. Run the Install Wizard to install any objects and policies for the new device, or create a new policy package.
5. If the new device uses an existing policy package, modify the Installation Targets of that package to include the new device and click *Install*.

Day-to-day management of devices

An administrator will often have to modify various objects for the devices they are responsible for managing. A typical set of tasks to manage an already provisioned device will include:

1. Adding, Deleting, or Editing various objects, such as firewall information, UTM profiles, User access rights, AV signatures, etc.
2. Adding, Deleting, or Editing all of the policy packages or individual policies within a policy package. This can include changing the order of operation, adding new policies or modifying information or access privileges in the policy package.
3. Installing updates to devices.

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.

Create a new policy package or folder

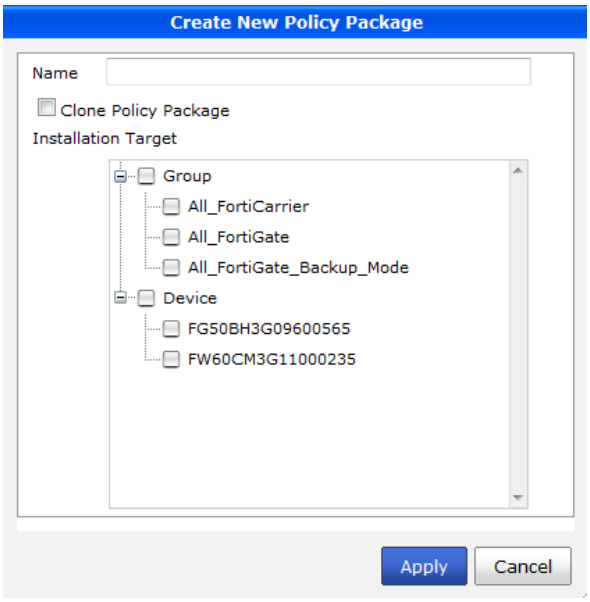
To create a new policy package or folder:

1. In the policy window of the navigation pane, right click on *Policy*.

Figure 116: Create new policy package

2. Select *New* > *Policy Package* to create a new policy package, or select *New* > *Folder* to create a new folder.

Figure 117: Enter new policy package details



3. Enter the desired name of the policy package or folder and, if creating a new policy package, if the package is cloned from a previous package select that package, and select the installation target or targets for the new package, then select *OK*.

Remove a policy package or folder

To remove a policy package or folder, right-click on the package or folder name in the navigation pane and select *delete* for the pop-up menu.

Rename a policy package or folder

To rename a policy package or folder, right-click on the package or folder name in the navigation pane and select *rename* for the pop-up menu. Enter the new name for the policy package or folder in the pop-up window and select *OK*.

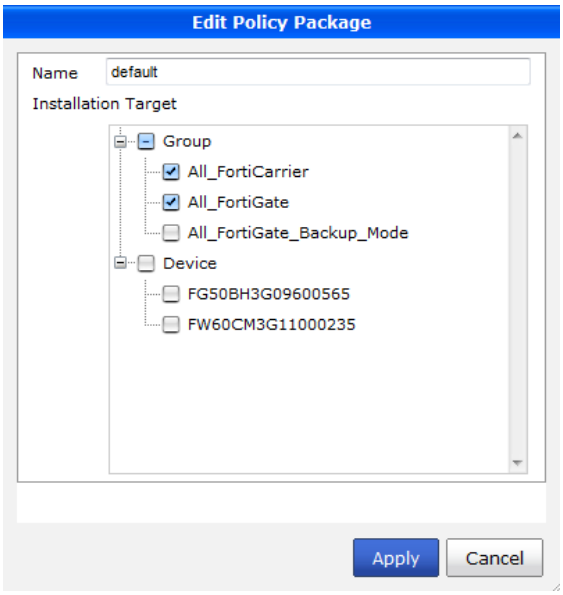
Install a policy package

To install a policy package to a target device:

1. In the policy window of the navigation pane, right-click on the requisite policy package and select *Edit*.

   The *Edit Policy Package* dialog box opens.

   Figure 118: Edit policy package dialog box



2. Select the devices or device groups to install the policy package onto and click *Apply*.

Perform a policy consistency check

Policy Check allows you to check all firewall policies to ensure consistency and eliminate conflicts that may prevent your devices from passing traffic. 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.

This allows you to optimize your policy sets and potentially reduce the size of your databases.

The Policy Check uses an algorithm to evaluate firewall 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.

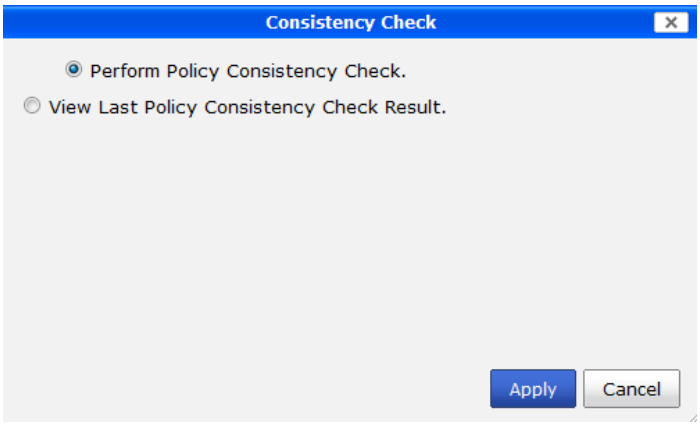
See Figure 121 on page 172.

To perform a policy check:

1. In the *Policy & Objects* tab, select Policy Check from the menu bar.

   The Consistency Check dialog box opens.

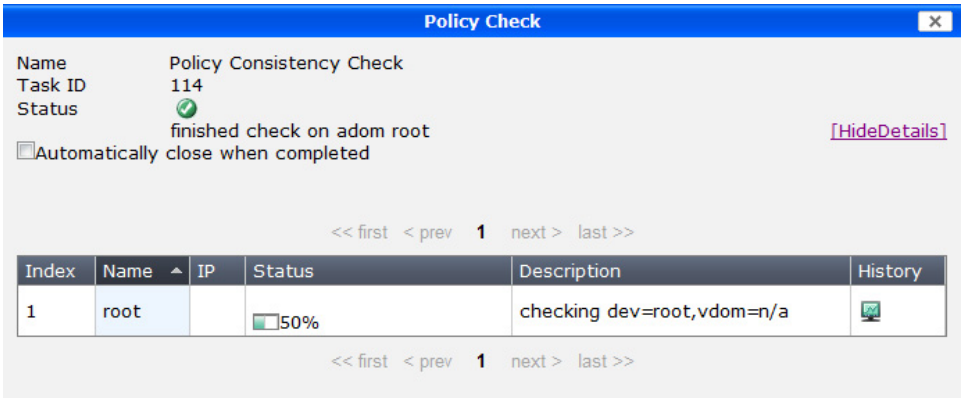
   Figure 119: Consistency Check dialog box



2. Select *Perform Policy consistency Check* and click *Apply*.

   A policy consistency check is performed and the results are displayed.

   Figure 120: Policy Check dialog box



To view the results of the last policy consistency check:

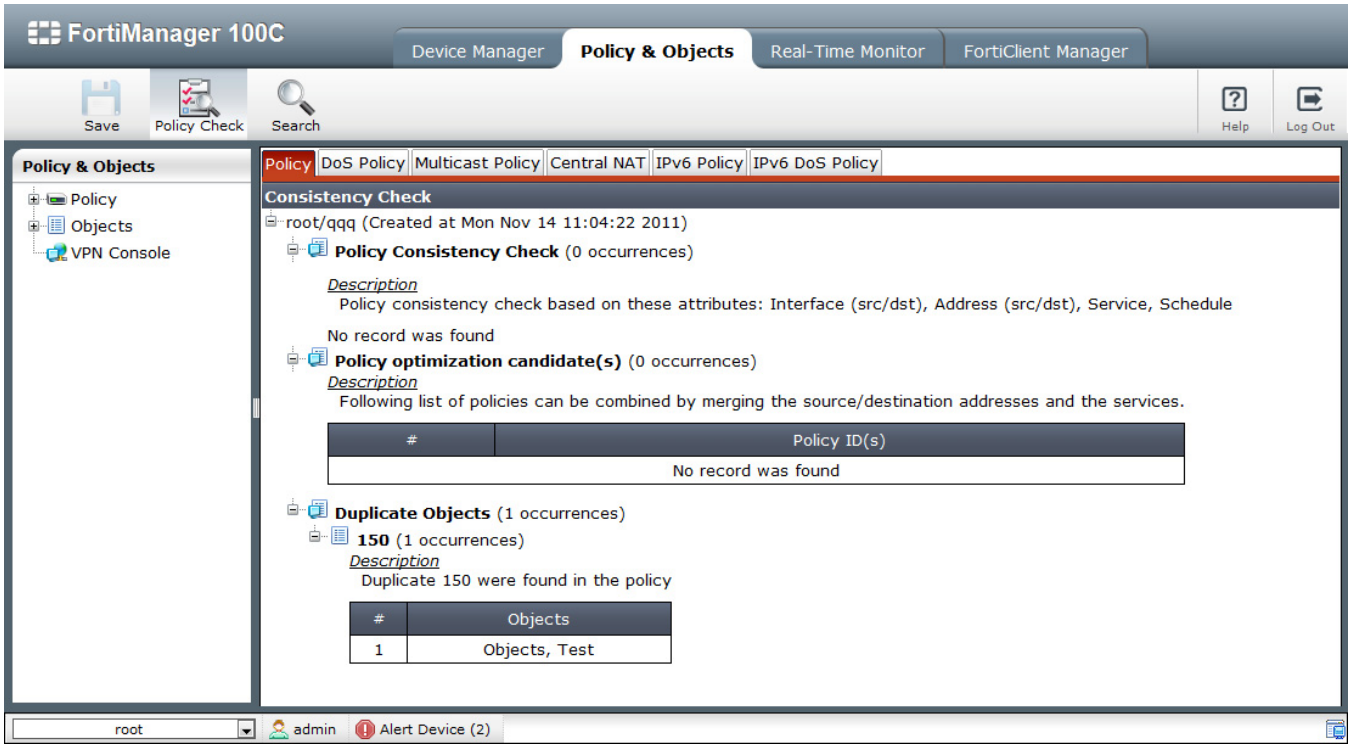
1. In the *Policy & Objects* tab, select Policy Check from the menu bar.

   The Consistency Check dialog box opens. See Figure 119.

2. Select *View Last Policy Consistency Check Results*. Click *Apply*.

   The Consistency Check window opens, showing the results of the last policy consistency check.

Figure 121: Consistency check results window



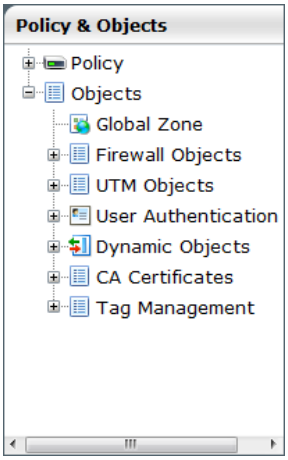
About objects and dynamic objects

All objects within an ADOM are managed by a single database unique to that ADOM. Objects inside that database can include items such as addresses, services, attack definitions, antivirus signatures, Web Filtering profiles, etc.

When making changes to an object within the object database, changes are reflected immediately within the policy table Web-based Manager. No copying to the database is required.

Dynamic objects are used to map a single logical object to a unique definition per device. For example, addresses, interfaces, virtual IPs and an IP pool can all be addressed dynamically.

Figure 122: Managing objects and dynamic objects



Managing objects and dynamic objects

The three global SSL VPN portal objects can be deleted, but can not be re-created. Reference bug ID 161981.

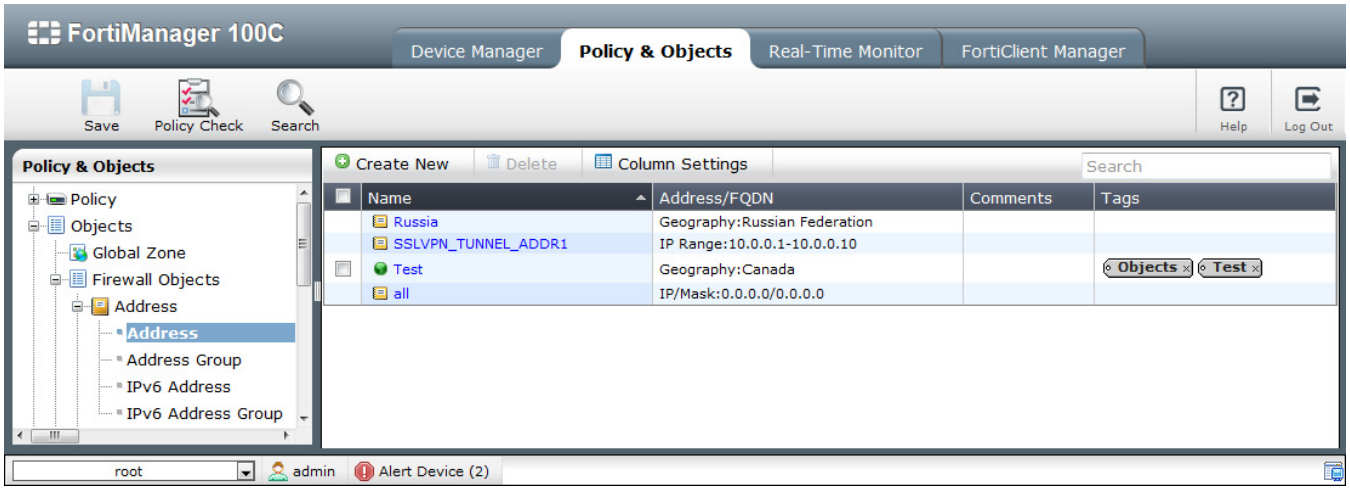
Create a new object or group

To create a new object:

1. Enter an ADOM and select the *Policy & Objects* tab. In the *Policy & Objects* window of the navigation pane, select an object. For example, a firewall address from *Firewall Objects* > *Address* > *Address*.

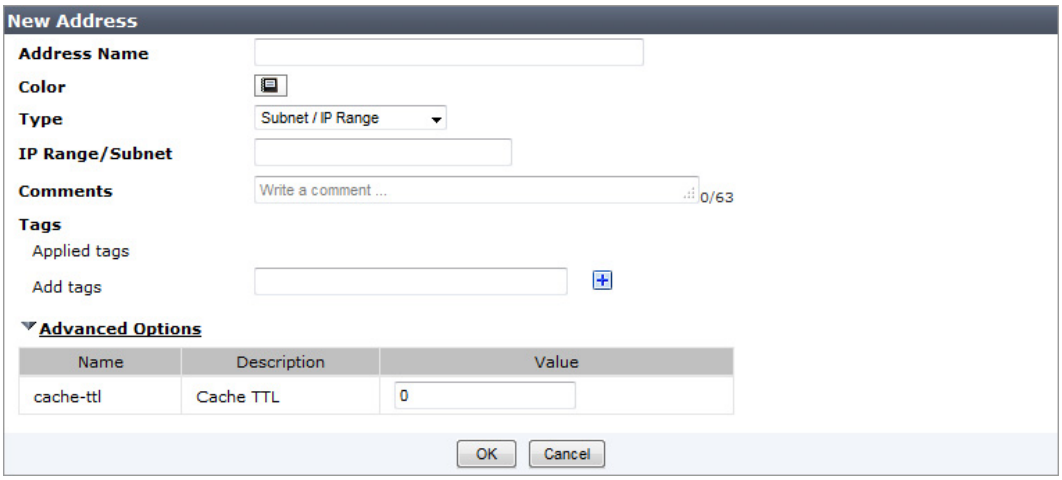
   The object list is displayed in the content pane.

Figure 123: Example object table



2. Select *Create New*.

Figure 124: Creating a new Firewall object address



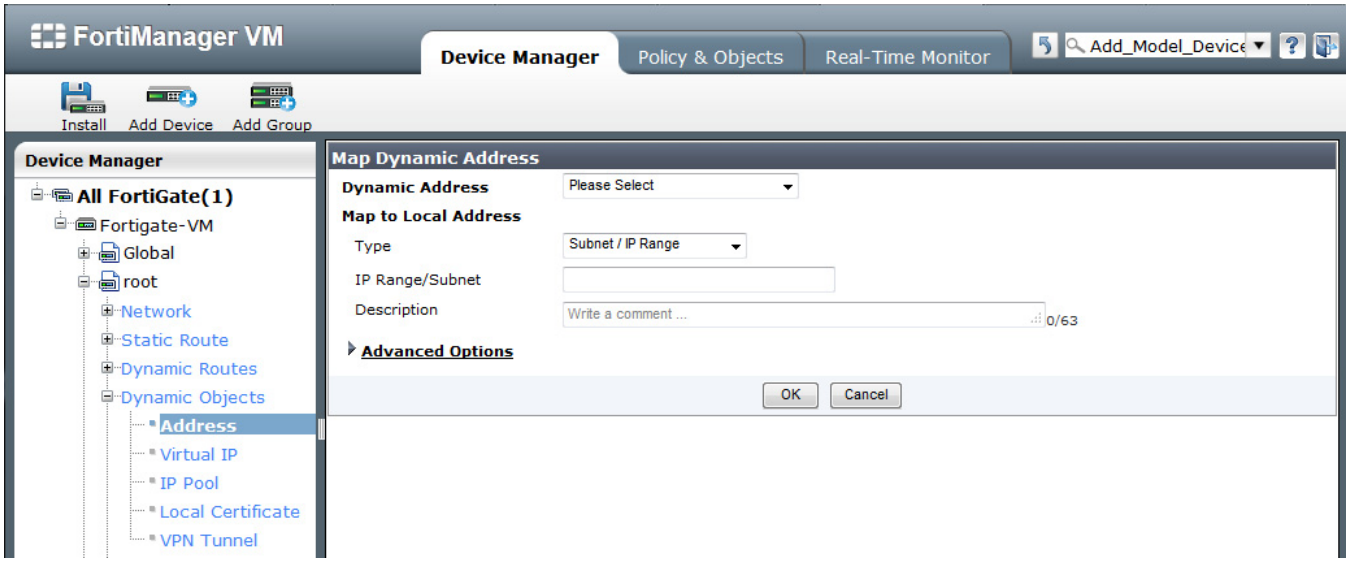
3. Enter the required information, depending on the object or object group selected.

4. Select *OK* to create the new object or object group.

Map the dynamic object

1. Select the *Device Manager* tab, and select the device from the left menu pane.
2. Select *Dynamic Objects* > *Address*, and then *Create New*.

Figure 125: Map dynamic address



3. Select the dynamic address object that you created in step 2, and map the *Dynamic Address* to a *Local Address*.

Remove an object or group

To remove an object or group, select the object and either click on the *delete* button, or right-click on the object name and select *delete* from the pop-up menu.

Edit an object or group

To edit an object:

1. In the navigation pane select *Objects* and locate the object or group that needs to be edited.
2. From the object or group list in the content pane, do one of the following:
   - Double-click on the name of the object or group to be edited
   - Right-click on the name of the object or group to be edited and select *Edit* from the pop-up menu.
3. Edit the information as required, and click *OK*.

Clone an object or group

If a new object or group is similar to a previously created object or group, the new object or group can be created by cloning the previous object or group.

To clone an object or group:

1. In the navigation pane select *Objects* and locate the object or group that is to be cloned.

2. Right-click on the object or group and select *Clone* from the pop-up menu.

   The *Edit* dialog box opens.
3. Change the information as required and select *OK* to create the new object or group.

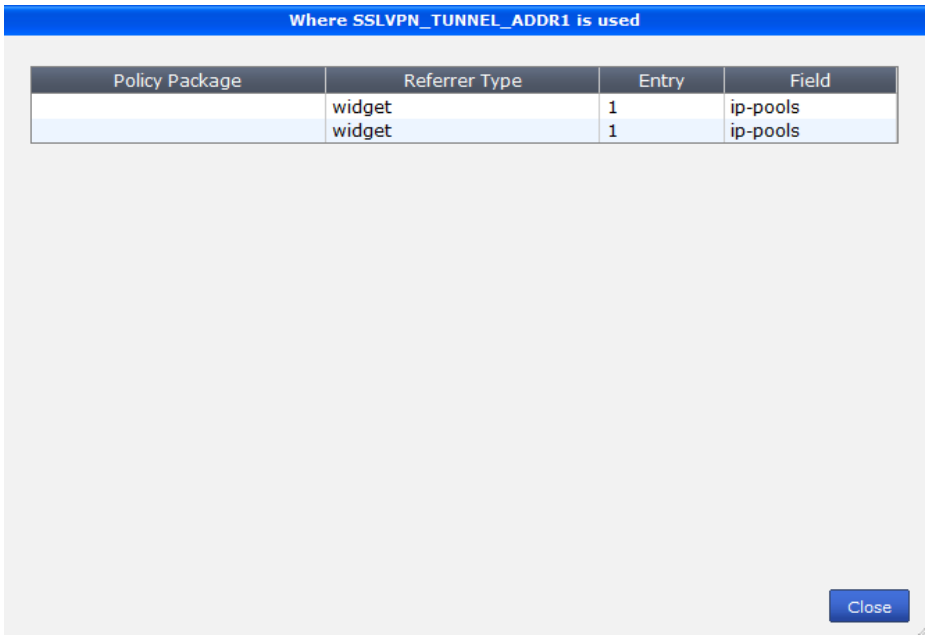
Search where an object or group is used

To determine where an object or group is being used:

1. In the navigation pane select *Objects* and locate the object or group.
2. Right-click on the object or group and select *Where Used* from the pop-up menu.

   The *Where Used* dialog box opens and displays the locations where the selected object or group is used; see Figure 126.

Figure 126: Where Used dialog box



Search objects

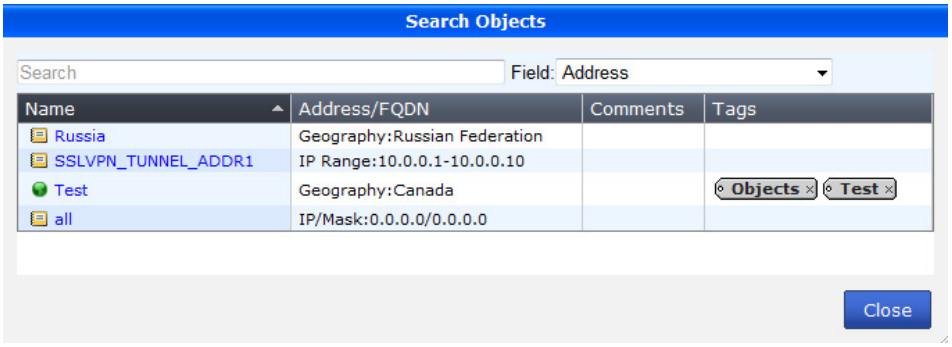
The search objects tool allows you to search objects based on keywords and field.

To search objects:

1. Select the *Policy & Objects* tab.
2. On the menu bar, select the search button.

   The search objects dialog box opens.

Figure 127: Search objects dialog box



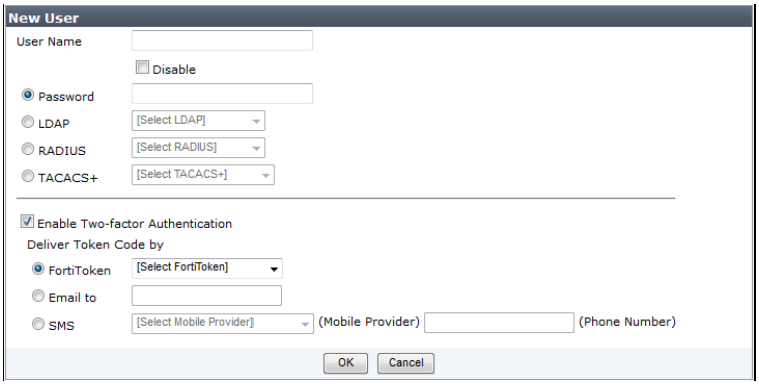
3. Enter a search keyword and select the field you would like to search.
4. The results of the search are displayed in the dialog box.

FortiToken configuration example

To configure FortiToken objects for FortiToken management, follow these steps:

1. On the FortiManager, select A*DOM* > *Policy & Objects* > *Objects* > *User Authentication* > *FortiToken*. Enter the serial number of the FortiToken unit and select *OK* to save the setting.
2. Select *ADOM* > *Policy & Objects* > *Objects* > *User Authentication* > *Local* and create a new user. Select *Enable Two-factor Authentication* and select the FortiToken from the drop down menu.

Figure 128: New local user window



3. Select *ADOM* > *Policy & Objects* > *Objects* > *User Authentication* > *User Group*. Create a new user group and add the user create in Step 2 to this group.
4. Install a policy package to the FortiGate.
5. On the FortiGate, select *User* > *FortiToken*. Select the FortiToken created in Step 1 and select to activate the FortiToken unit.

VPN Console

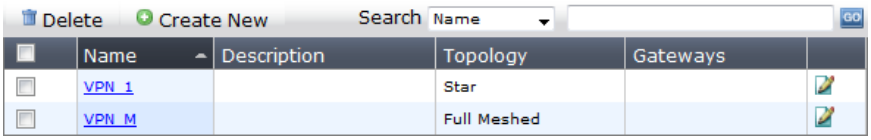
The VPN Console enables you to create VPN topology configurations and copy them to the managed FortiGate units. To see the list of VPN configurations, go to *VPN Console* in the navigation pane of the *Policy & Objects* tab.

To access the VPN Console, VPN consoles must be enabled. See "Enable or disable VPN consoles" on page 178.

When you have a VPN Console in the content pane list, selecting the name of that entry will take you to a new screen. From there you can create gateways and subnets for that VPN console. These are required if you configure a VPN Policy and select *Specify Source/Destination Protected Subnets* for the *Policy Scope*. See "Create VPN firewall policies" on page 185.

There is no right-click menu available for the VPN console list.

Figure 129:VPN list



The following information and options are available

Delete	To delete a VPN configuration, select one or more configurations from the list by selecting its check box, then select *Delete*.
Create New	Create a new VPN configuration.
Search	To locate a VPN configuration, select a search criteria from the drop down list box, enter the keyword text in the text box beside and select *Go*.
Check Box	Select one or more VPN Console entries to delete.
Name	The VPN name.
Description	Optional description.
Topology	One of: *Full Meshed* — each gateway has a tunnel to every other gateway *Star* — each gateway has one tunnel to a central hub gateway *Dialup* — some gateways, often mobile users, have dynamic IP addresses and contact the gateway to establish a tunnel
Gateways	The FortiGate units that function as the VPN tunnel ends.
Edit icon	Edit this VPN configuration.

Configuring a VPN

To create a VPN, you need to:

- Enable VPN Console connections.
- Create firewall addresses for your VPN's protected subnets.
- Create the VPN configuration.
- Add VPN gateways.
- Create VPN firewall policies in the Policy Console.

Enable or disable VPN consoles

VPN console connections can be enabled or disabled on the *Edit ADOM* page. See "Managing ADOMs" on page 41.

When enabled, the VPN console is a central management module that controls all of the VPNs within the ADOM. When the VPN Console is disabled, you can configure VPN console connections in device manager, and in the policy console for policy-based IPsec.

To enable or disable the VPN Console:

1. In the navigation pane, select *Global* from the ADOM drop-down menu.
2. Select *Administrator Domain* in the navigation pane.
3. Double-click, or right-click and select edit, on the domain you want to configure. A dialog box appears.
4. To enable the VPN Console, deselect *No VPN Console*.

   To disable the VPN Console, select *No VPN Console*.
5. When done, select *OK*.

Create a firewall address

Ensure the port needed to begin or end the VPN tunnel is setup with a valid IP address and network mask. These addresses will be used by the firewall policy for the source and destination addresses of the VPN policy.

To create a firewall address:

1. Go to *Objects* > *Firewall Objects* > *Address* > *Address*.
2. Select *Create New*. See Figure 122 on page 172.
3. Enter the port address information and select *OK*.

Create a VPN configuration

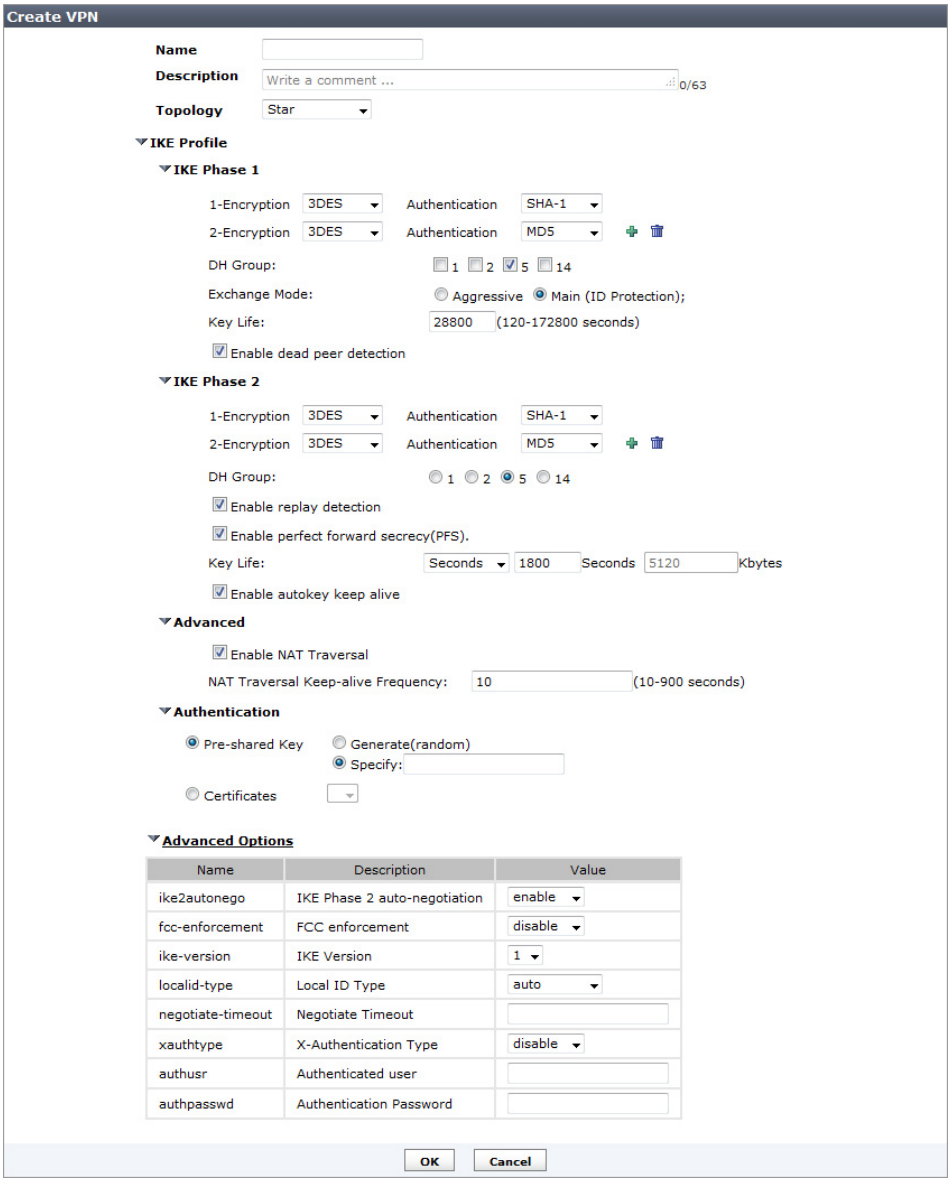
The VPN configuration defines the structure of the VPN tunnel. It includes the type of tunnel to create, and the encryption/security level to apply to the tunnel. The configuration you create in the steps below are applied in the VPN firewall policy.

To create a VPN configuration:

1. Go to *VPN Console*.
2. Select *Create New.*

   The create new VPN window appears.

Figure 130: Create VPN window



3. Configure the following settings:

Name	Enter a name for the new VPN configuration.
Description	Enter a tunnel description. (Optional)
Topology	Choose from Full Mesh, Star, or Dial up.
IKE Profile	Create Phase 1 and Phase 2 configurations.
IKE Phase 1	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.

1-Encryption **2-Encryption** **Authentication**	Select one of the following symmetric-key encryption algorithms: • DES — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • 3DES — Triple-DES, in which plain text is encrypted three times by three keys. • AES128 — a 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key. • AES192 — a 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key. • AES256 — a 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key. 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.
Exchange Mode	Select Main (ID Protection) or Aggressive: • Main mode — the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information. • Aggressive mode — the phase 1 parameters are exchanged in single message with authentication information that is not encrypted. When the remote VPN peer has a dynamic IP address and is authenticated by a pre-shared key, you must select Aggressive mode if there is more than one dialup phase1 configuration for the interface IP address. When the remote VPN peer has a dynamic IP address and is authenticated by a certificate, you must select Aggressive mode if there is more than one phase 1 configuration for the interface IP address and these phase 1 configurations use different proposals.

Key Life	Enter 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 172 800 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.
IKE Phase 2	
1-Encryption **2-Encryption** **Authentication**	Select one of the following symmetric-key encryption algorithms: • DES — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • 3DES — Triple-DES, in which plain text is encrypted three times by three keys. • AES128 — a 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key. • AES192 — a 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key. • AES256 — a 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key. 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.
Enable 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)	Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.

Key Life	Enter 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 172 800 seconds.
Enable autokey keep alive	Select the check box if you want the tunnel to remain active when no data is being processed.
Enable auto-negotiation	When enabled, auto-negotiate initiates the phase 2 SA negotiation automatically, repeating every five seconds until the SA is established.
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, enter a keepalive frequency setting.
Authentication	
Pre-shared Key	If you selected Pre-shared Key, enter 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.
Certificates	If you selected RSA Signature, 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.
Advanced Options	
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.
Local ID Type	Select auto, fqdn, user-fqdn, keyid, address, or asn1dn from the drop-down menu.
Negotiate Timeout	Enter a numerical value for the negotiate timeout period.

4. Enter a name and description for the VPN.
5. Select the VPN *Topology* to use.
6. Enter the *IKE Phase 1*, *IKE Phase 2*, *Advanced*, and *Authentication* settings.

   For *Pre-shared Key*, select *Generate (random)* or select *Specify* and enter the key.
7. If required, select *Advanced Options* to configure advanced options.
8. Select *OK*.

Add a VPN gateway

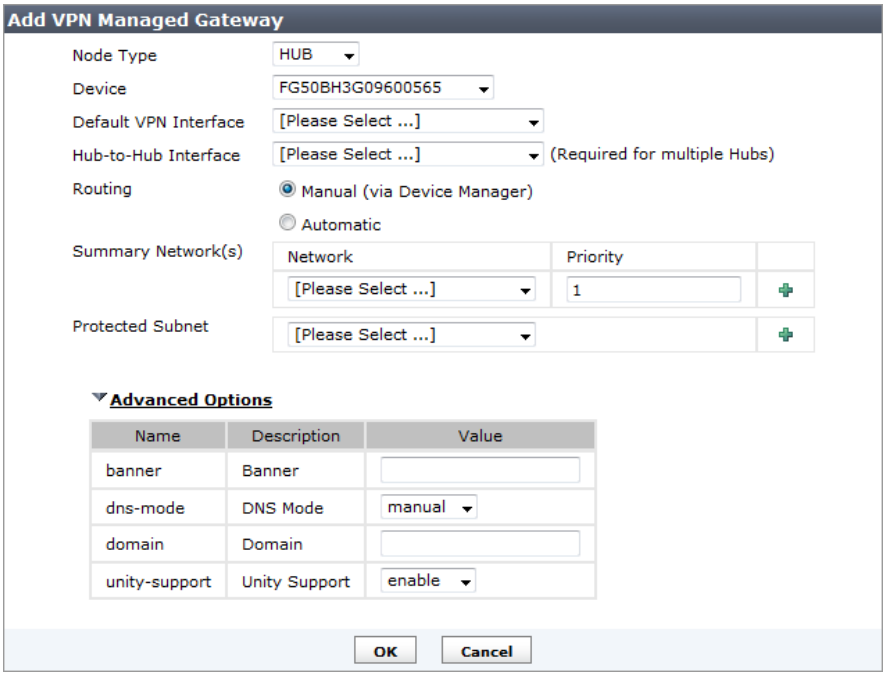
Create a VPN gateway. This is the address/port combination the VPN tunnel will use to route traffic.

You must set one or more Protected Subnets for the VPN Console to be able to select *Specify Source/Destination Protected Subnet* under the *Policy Scope*. If you do not, the list will be empty and you will have to select *Apply to Traffic between All Protected Subnets* instead. See "Create VPN firewall policies" on page 185.

To add a Managed VPN gateway:

1. Go to *VPN Console*.
2. In the content pane VPN list, select the name of a VPN Console entry.
3. Select *Create New* and choose *Managed Gateway* from the drop-down list.

Figure 131: Add VPN Managed Gateway dialog box



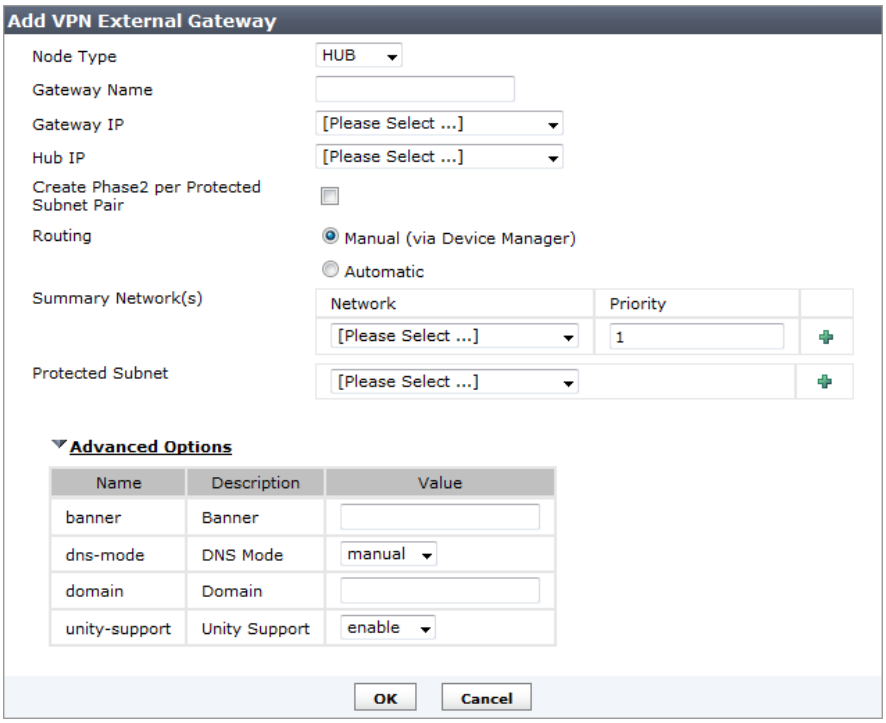
4. Select the *Node Type* as one of HUB or Spoke.
5. Select the *Device* for the VPN gateway. This device must already exist in the FortiManager database. To add new devices, see "Adding a device" on page 142.
6. Select the *Default VPN Interface* on the VPN device that connects the VPN to the public network.
7. Select the routing options. Select *Manual* to create the route yourself in *Device manager* or select *Automatic* for the VPN console to automatically configure the interface on the VPN device that connects the VPN to the public network.
8. Select the *Summary Networks* by selecting the configured interface and firewall address for that network and then select the plus ("+") icon to apply the entry. Repeat for each summary network.
9. Select the *Protected Subnet* by selecting the configured interface and firewall address for that network and then select the plus ("+") icon to apply the entry. Repeat for each protected subnet.

10. If required, adjust the advanced options.
11. Select *OK*.

To add an External VPN gateway:

1. Go to *VPN Console*.
2. In the content pane VPN list, select the name of a VPN Console entry.
3. Select *Create New* and choose *External Gateway* from the drop-down list.

Figure 132: Add VPN External Gateway dialog box



4. Select the *Node Type* as one of HUB or Spoke.
5. Select the *Device* for the VPN gateway. This device must already exist in the FortiManager database. To add new devices, see "Adding a device" on page 142.
6. Select the *Default VPN Interface* on the VPN device that connects the VPN to the public network.
7. Select the routing options. Select *Manual* to create the route yourself in *Device manager* or select *Automatic* for the VPN console to automatically configure the interface on the VPN device that connects the VPN to the public network.
8. Select the *Summary Networks* by selecting the configured interface and firewall address for that network and then select the plus ("+") icon to apply the entry. Repeat for each summary network.
9. Select the *Protected Subnet* by selecting the configured interface and firewall address for that network and then select the plus ("+") icon to apply the entry. Repeat for each protected subnet.
10. If required, adjust the advanced options.
11. Select *OK*.

Create VPN firewall policies

Create the firewall policies that allows the network traffic through the FortiGate units completing the tunnel.

To create VPN firewall policies:

1. Go to *Policy & Objects* > *Policy*.
2. Right click on *Policy* in the navigation pane and select *New* > *Policy Package*.
3. Enter a name for the policy package and select the *Installation Target* and select *Apply*.
4. Select the Policy Package in the navigation pane and right click Local Domain Policies. Select *Create New* > *Policy*.
5. Define the *Source Zone, Destination, Destination Zone, Destination Address, Schedule, Service, Action*.

   If you select *Specify Source/Destination Protected Subnets*, you must select the source and destination device and subnets from the VPN gateway *Protected Subnets* configured in "Add a VPN gateway" on page 183.
6. Configure *Logging* and *Advanced Options* fields as required.
7. Select *OK*.

Installing Device Configurations

The FortiManager system maintains a configuration repository to manage device configuration revisions. After modifying device configurations, you can save them to the FortiManager repository and install the modified configurations to individual devices or device groups. You can also retrieve the current configuration of a device, or revert a device's configuration to a previous revision.

This section contains the following topics:

- Checking device configuration status
- Managing configuration revision history

Checking device configuration status

In the *Device Manager* window, when you select a device, you can view that device's basic information under the *Summary* tab. You can also check if the current configuration file of the device stored in the FortiManager repository is in sync with the one running on the device.

If you make any configuration changes to a device directly, rather than using the FortiManager system, the configuration on the device and the configuration saved in the FortiManager repository will be out of sync. In this case, you can resynchronize with the device by retrieving the configuration from the device and saving it to the FortiManager repository.

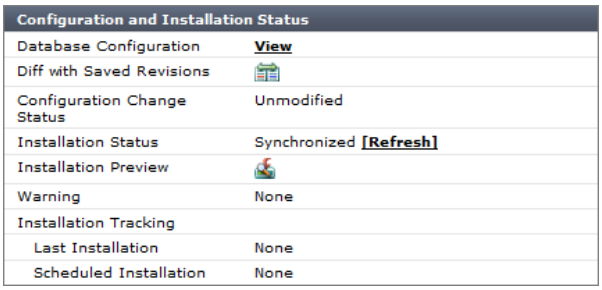
You can use the following procedures when checking device configuration status on a FortiGate, FortiSwitch, FortiCarrier, or FortiMail unit.

To check the status of a configuration installation on a FortiGate unit:

1. Go to *Device Manager* > *FortiGate*.
2. On the All FortiGate page, select the FortiGate unit that you want to check the configuration status of.

   You are automatically redirected to *System* > *Dashboard* > *Status* of that unit.
3. On the Status page, locate the Configuration and Installation Status widget.
4. Verify the status in the *Configuration Change Status* row.

Figure 133: Configuration and Installation Status widget



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

To view the device installation history on a FortiGate unit:

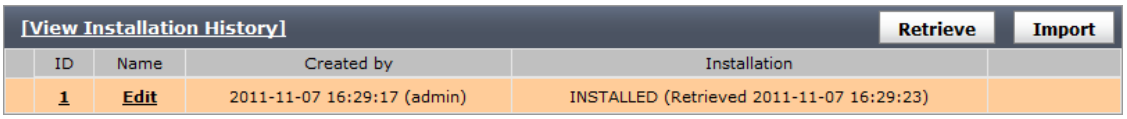
1. In the navigation pane, select *Revision History*.
2. Select *View Installation History*.

   You are automatically redirected to the View Installation History page.

Managing configuration revision history

In the *Device Manager* window, select a device in the device tree and then select the *Revision History* tab to view the FortiManager repository.

Figure 134: Revision history tab



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 189.
Comments icon	Display the comment added to this configuration file when you edit the file name.
ID	A number assigned by the FortiManager system to identify the version of the configuration file saved on the FortiManager repository. Select an ID to view the configuration file. You can also select the Download button to save this configuration file from the FortiManager system to a local computer. See "To view the configuration settings on a FortiGate unit:" on page 188 and "To download a configuration file to a local computer:" on page 189.
Name	A name added by the user to make it easier to identify specific configuration versions. You can select a name to edit it and add comments.
Created by	The time and date when the configuration file was created, and the person who created the file.

Installation	Display whether a configuration file has been installed or is currently active. The installation time and date is displayed. N/A status indicates that a particular revision was not sent to the device. The typical situation is that the changes were part of a later revision that was sent out to the device. For example, you make some changes and commit the changes. Now you have a revision called ID1. Then you make more changes and commit the changes again. Then you have a revision called ID2, which also includes the changes you made in revision ID1. If you install revision ID2, then the status of revision ID1 becomes N/A.
Diff icon	Show only the changes or differences between two versions of a configuration file. See "Comparing different configuration files" on page 189 for more details.
Delete icon	Delete this version from the repository. You cannot delete a version that is currently active on the FortiGate unit.
Revert icon	Revert the current configuration to the selected revision. FortiManager tags the reverted configuration with a new ID number. For example, if you are currently running version 9 and revert to version 8, a new revision, version 10, is created at the top of the list. See "To revert to another configuration file:" on page 190.

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

To view the configuration settings on a FortiGate unit:

1. In the navigation pane with a device already selected, go to *System* > *Status* > *Dashboard* > *Revision History*.
2. Select the *ID* for the revision you want to see.

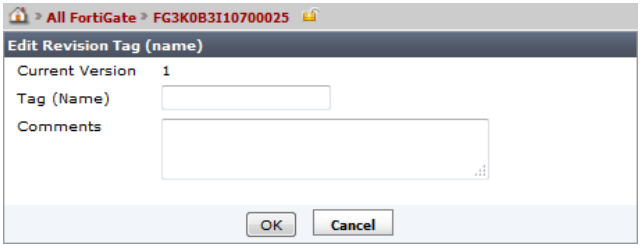
   You are automatically redirected to the View Configuration page.
3. Select *Return* when you finish viewing.

You can download the configuration settings if you want by selecting Download on the View Configuration page. For more information, see "Downloading and importing a configuration file" on page 189.

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

1. In the navigation pane with a device already selected, go to *System* > *Status* > *Dashboard* > *Revision History*.
2. Select the *Name* for the version you want to change.
3. Enter a name in the *Tag (Name)* field.
4. Optionally, enter information in the *Comments* field.
5. Select *OK*.

Figure 135: Add a tag to a configuration version



Downloading and importing a configuration file

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

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

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

To download a configuration file to a local computer:

1. In the navigation pane with a device already selected, go to *System* > *Status* > *Dashboard* > *Revision History*.
2. Select the *ID* for the revision you want to download.
3. Select the *Download* button.

   You may need to drag the scroll bar to the very right to see the button.
4. Select *Regular* or *Encrypted* download type. If you select *Encrypted Download*, enter a password.
5. Select *OK*.
6. Specify a location to save the configuration file on the local computer.
7. Select *Save*.

To import a configuration file from a local computer:

1. In the navigation pane with a device already selected, go to *System* > *Status* > *Dashboard* > *Revision History*.
2. Select *Import*.
3. Select the location of the configuration file or choose *Browse* to locate the file.
4. If the file is encrypted, select the *File is Encrypted* check box and enter the password.
5. Select *OK*.

Comparing different configuration files

You can compare the changes or differences between two versions of a configuration file by using the Diff function.

The Diff function behaves differently under certain circumstances.

For example, when a device is first added to the FortiManager system, the FortiManager system gets the configuration file directly from the FortiGate unit and stores it as is. This configuration file is version/ID 1.

If you make changes to the device configuration on *Device Manager* Configuration tab and select Commit, the new configuration file will be saved as version/ID 2. If you use the Diff icon to view the changes/differences between version/ID 1 and version/ID 2, you will be shown more changes than you have made.

This happens because the items in the file version/ID 1 are ordered as they are on the FortiGate unit. Configurations of version/ID 2 are sequenced differently when they are edited and committed in the *Device Manager*. Therefore, when you compare version/ID 1 and version/ID 2, the Diff function sees every item in the configuration file as changed.

If you take version/ID 2, change an item and commit it, the tag is changed to version/ID 3. If you use Diff with version/ID 2 and version/ID 3, only the changes that you made will be shown. This is because version/ID 2 and version/ID 3 have both been sequenced in the same way in the *Device Manager*.

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

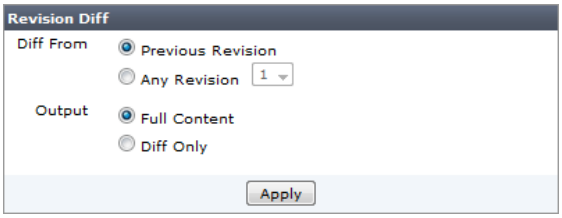
To compare different configuration files:

1. In the navigation pane with a device already selected, go to *System* > *Dashboard* > *Status*.
2. On the Status page, locate the Configuration and Installation Status widget.
3. In the *Diff with Saved Revisions* row, select the *Revision Diff* icon,  .
4. Select either the previous version or specify a different configuration version to compare in *Diff From*.
5. Select whether to display the full configuration file (*Full Content*) or only the differences (*Diff Only*) in *Output*.

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

   The configuration differences are displayed in colored highlights:

   Figure 136: Revision Diff window



To revert to another configuration file:

1. In the navigation pane with a device already selected, go to *System* > *Status* > *Dashboard* > *Revision History*.
2. Select the *Revert* icon for the revision you want to revert to.
3. Select *OK*.

   A new revision is added to the top of the list.

Advanced Features

FortiManager offers users certain advanced features which are obtainable through an upgrade to your current FortiManager license.

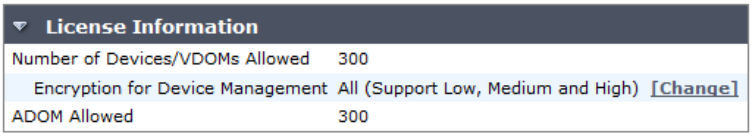
Upgradable license features include:

- Fortinet Developer Network
- ADOM upgrade (FMG_VM)

In FortiManager v4.0 MR3 Patch Release 8 the following advanced features are supported without additional licensing:

- Global policy
- Web portal

Figure 137: License information widget



About global policies and objects

Global policies and objects function in a similar fashion to the policies and objects you are already familiar with, 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.

Assigning global policies to ADOMs

FortiManager v4.0 MR3 allows administrators to assign a global policy or global database to more than one ADOM. This enhancement provides a finer granularity to assign specific policy packages within each ADOM.

Searching for global objects content

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

Currently, you can search for the following global objects:

Address	Recurring Schedule	Antivirus Profile
Address Group	One-time Schedule	Web Filter Profile
Service	Schedule Group	Spam Filter Profile
Service Group	Protocol Options	VoIP Profile

To search, select *Search* from the main menu bar. On the search screen, enter the following information.

Search for	Select the global object that you want to search.
Search Criteria	Select the value upon which the search is based.
Object by Name	*Object by Name*: This option is available for all object types in the *Search for* field. If you select this option, enter the object name and select a matching method: *Exact Match*: Select to require that matching object must be the same as the object name entered. This is case sensitive. If an object name does not match the object name entered, it will not be included in the search results. *Starts With*: Select to require that matching object must start with a letter (case sensitive) or word at the beginning of the object name entered. For example, you can enter A to search for Addr1. *Regular Expression*: Select to search with wildcards or Perl regular expressions. See http://perldoc.perl.org/perlretut.html for detailed information about using Perl regular expressions.
Object by Value	*Object by Value*: This option is available only when you select *Address* or *Service* in the *Search for* field. If you select *Address* in the *Search for* field and then *Object by Value* in the *Search Criteria* field, select the value type (*IP Address/Range* or *FQDN*) and enter the IP or FQDN in the *Address* field. You can use the exact match or regular expression to enter the IP or FQDN. For information on IP search rules, see "IP address search rules" on page 193. If you select *Service* in the *Search for* field and then *Object by Value* in the *Search Criteria* field, select a protocol and enter the corresponding information for the protocol.

Unused Objects	*Unused Objects*: This option is available for all object types in the *Search for* field. This option is typically used by system administrators on a periodic basis to clean up the system. Over time, more and more objects are added to the system and then removed from policies or other uses. However, they still exist in the FortiGate configuration. There are no additional search parameters required for this option.
Object Usage	*Object usage*: This option is available for all object types in the *Search for* field. This option is typically used by system administrators to identify where an object is being used, that is, which policy or device is using it. There are no additional search parameters required for this option.
Scope	Specify the search scope for an object. To access additional scope information, including *Search All ADOMs* and *Narrow Search Parameters* options, select *more* >>. To hide these options select << *Less*. When you select *Object by Name*, *Object by Value*, or *Unused Objects* in the *Search Criteria* field, after entering the search criteria, you can search an object globally or narrow the search by selecting an ADOM. • *All Databases*: Select to search all databases in the FortiManager system. You can also select *Search All ADOMS* to search the databases of each ADOM. • *Narrow Search Parameters (optimized)*: If you know which ADOM the object is in, select this option to save search time. You can select the *ADOM*, the *Global Database*/*Security Console* of the ADOM, or a particular *Device* or *Group* of the ADOM. For more information, see "To search an object by name:" on page 194, "To search an object by value:" on page 195, and "To search an unused object:" on page 196. When you select *Object Usage* in the *Search Criteria* field, you can find out where an object is being used, that is, which policy or which device is using it. For more information, see "To search an object by usage:" on page 196.

IP address search rules

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

The following examples explain the IP address search rules.

Assuming that we have the following IP address definitions:

#	IP Address/Mask or IP Range
1	192.169.10.1/32
2	192.169.10.0/24
3	192.169.0.0/16

4	192.169.10.1-192.169.10.9
5	192.169.10.10-192.169.10.19

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

To search an object by name:

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

   The search result displays the following information:

Delete	Select the check box beside an address that you want to delete, then select *Delete* to remove it. If there is no check box beside an address, it means that this address is used by an address group.
New Search	Select to start a new search.
Name	The name of an address.
Address/FQDN	The IP address/mask of the address.
Detail	Any comments added for the firewall address.
ADOM	The ADOM that this address is in. For information about ADOMs, see “Administrative Domains” on page 38.

Device (VDOM)	The database where this address is saved.
Filter	Display the devices and groups that can use the global firewall address configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration.

To search an object by value:

1. From the Main Menu Bar, select *Search*.
2. In the *Search for* field, select *Address* or *Service*.
3. In the *Search Criteria* field, select *Object by Value.*
4. Do one of the following:
   - If you selected *Address* in the *Search for* field, select the value type (*IP Address/Range* or *FQDN*) and enter the IP or FQDN in the *Address* field. You can use the exact match or regular expression to enter the IP or FQDN.
   - If you selected *Service* in the *Search for* field, select a protocol and enter the corresponding information for the protocol following the table.

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

5. Repeat step 5 in "To search an object by name:" on page 194.
6. Select *Search*.

   The search result displays.

Delete	Select the check box beside a service that you want to delete, then select *Delete* to remove it. If there is no check box beside a service, it means that this service is used by a service group.
New Search	Select to start a new search.
Service Name	The name of the firewall service.
Detail	The protocol and port numbers for each service.
ADOM	The ADOM that this service is in. For information about ADOM, see "Administrative Domains" on page 38.

Device (VDOM)	The database where this service is saved.
Filter	Display the devices and groups that can use the global firewall service configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration.

To search an unused object:

1. From the Main Menu Bar, select *Search*.
2. In the *Search for* field, select an object.
3. In the *Search Criteria* field*,* select *Unused Objects.*
4. Repeat step 5 in "To search an object by name:" on page 194.
5. Select *Search*.

   The search result displays the following:

Delete	Select the check box beside a profile that you want to delete, then select *Delete* to remove it. If there is no check box beside a profile, it means that this profile is used by a firewall policy.
New Search	Select to start a new search.
Name	The name of the protection profile.
ADOM	The ADOM that this service is in. For information about ADOM, see "Administrative Domains" on page 38.
Device (VDOM)	The database where this profile is saved.
Filter	Display the devices and groups that can use the global protection profile configuration. If specific devices and/or groups are listed, it means that these devices and groups are allowed to use the configuration. If *All Devices/Groups* displays, it means that all devices and groups are allowed to use the configuration.

To search an object by usage:

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

The search result displays the following:

New Search	Select to start a new search.
ADOM	The ADOM that this address is in. For information about ADOM, see “Administrative Domains” on page 38.
Device (VDOM)	The database where this address is saved.
Referrer Type	The type of object that uses this address. In this case, the type is firewall address groups.
Entry	The name of the firewall address group that uses this address.
Field	The nature of the address in the address group, such as being added as a group member.

The three global SSL VPN portal objects can be deleted, but can not be re-created. Reference Mantis Bug ID 161981.

Configuring web portals

The web portal enables MSSP customers to manage their own SSL VPN user list, web filter, URL filters, and categories. If configured, customers can also view the firewall policies on their FortiGate devices or VDOM.

You create a portal profile and include its content and appearance. You can then create more profiles if customers have differing needs. The portal is composed of selected configuration and monitoring widgets, on one or more pages, to provide the specific functionality that the administrators need to monitor their network security. You can also customize the web portal with a logo and select the colors and page layouts for your business, or match the customer’s corporate look. With FortiManager, you define each customer/administrator as a portal user, assigned to a specific portal profile.

Using FortiManager, you can maintain a number of FortiGate units and/or VDOMs for a large number of clients. These clients may also want to monitor and maintain their own firewall policies and traffic.

Customers access the web portal through the IP or URL of the FortiManager system. They log in the same way as the FortiManager administrator, using their own user name and password, created by the FortiManager administrator. Once logged in, the customer is directed to their assigned web portal. The customer does not have access to the FortiManager Web-based Manager.

To create a web portal for customers to access, you need to first create a portal profile. A web portal is similar to a group. The profile is associated with a FortiGate unit, and if required, a VDOM configured on a specific FortiGate unit. Once set up, portal users, or administrators, can be added to the portal.

The following table lists the number of supported portals and portal users on each FortiManager model.

Table 9: Supported web portals and web portal users

FortiManager Model	Maximum portal	Maximum users
FMG-100B, FMG-100C, FMG-200D	not supported	not supported
FMG-400A, FMG-400B, FMG-400C	not supported	not supported
FMG-1000B	50	500
FMG-1000C	50	500
FMG-3000	50	500
FMG-3000B	100	4000
FMG-3000C	100	4000
FMG-5001A	100	4000

After creating a web portal, you can configure it to add components that the user or administrator can review and modify as required. You can return at anytime to add and remove components from the portal. It is a good idea to meet or discuss with your users which components they would like to see on their portal. Provide them a list of what options they have, and allow them to select from the list.

The web portal can also be customized to a selection of color schemes, and you can add a user's logo to make the portal to fit the customer's corporate look. Users are not able to modify the layout or look of the web portal, although they can add and modify the content of some of the components. For example, they can add SSL VPN users, modify URL filter lists, and add text notes. If they require changes to the components (adding or removing) or the layout of the components on the portal page, they will need to contact you.

Creating a web portal

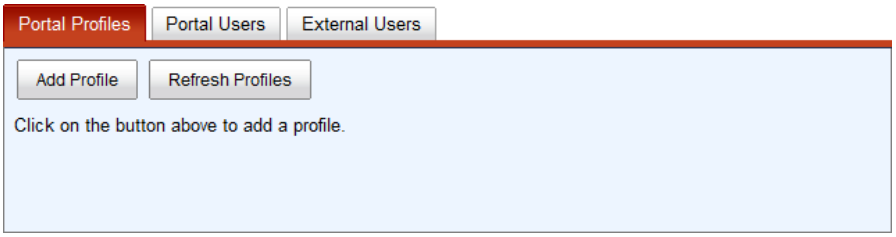
Before creating a web portal, ensure you have the FortiGate configured and any VDOMs enabled and configured. You may also want to discuss with your user as to what components they want or required for their portal.

To create a web portal profile:

1. Go to *Device Manager* > *Tools* > *Web Portal*.

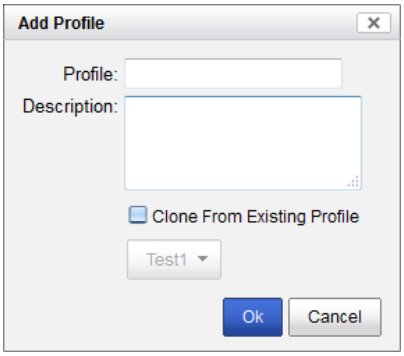
Show Web Portal must be selected in the Admin Settings. See "Configuring global admin settings" on page 93 for more information.

Figure 138: Web Portal Window



2. Select *Add Profile*.

Figure 139: Add profile dialog box



3. In the *Profile* field, enter a name for the profile, and optionally, enter a *Description*.
4. If you have already added a portal profile you can select *Clone from existing profile* to add the new profile using the settings from a previously added profile.
5. Select *OK*.

The *Profile* name can be a maximum of 35 characters.

Configuring the web portal profile

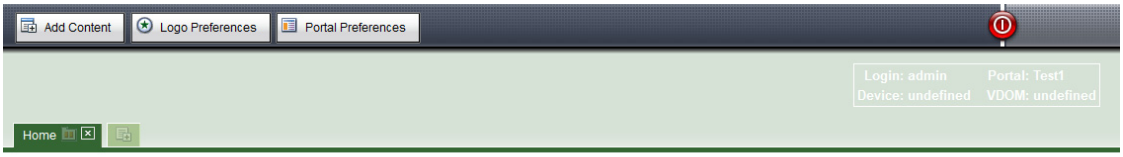
With the web portal added, you can configure the portal with the available widgets. The selection of widgets are dependent on the FortiGate device and VDOM (if selected), that is, you may have more or less widgets available to choose from depending on the FortiGate device selected for the portal. The selected device is only used for assistance. The device or VDOM is defined when creating the user.

To configure the web portal profile:

1. Go to *Device Manager* > *Tools* > *Web Portal*.
2. Select a profile from the list.
3. Select the *Configure Profile* icon for the profile.
4. Select *Configure Profile*.

When you select *Configure Profile*, the web portal design window opens in a new window or tab of the browser. You may need to allow pop ups for the FortiManager IP or URL to allow the portal design window to appear, otherwise this window will not appear.

Figure 140: Blank web portal window



Modifying the content and layout

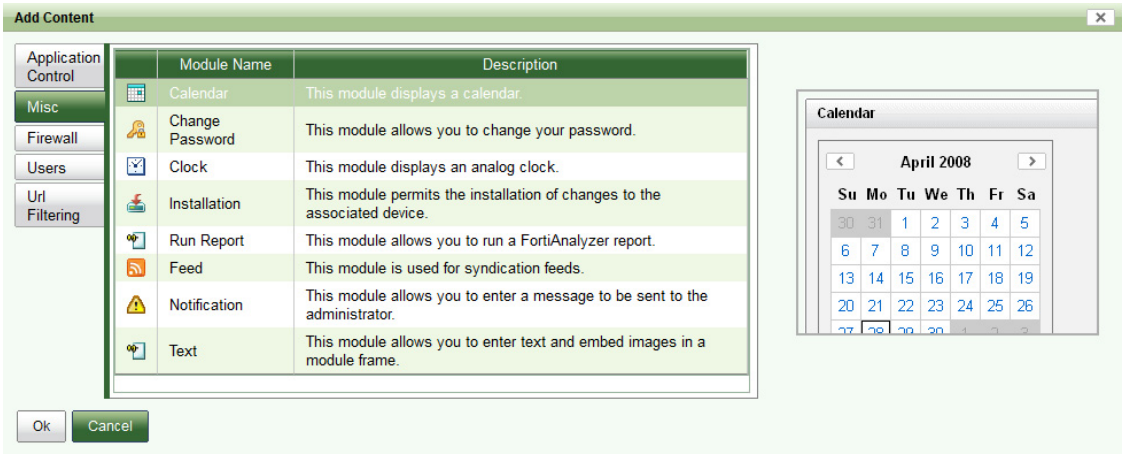
The web portal design window enables you to add content for the user's internet and firewall connection and arrange the layout of the information.

Before adding widgets for the portal, you will want to set up the portal window. There are a number of customizations you can do to the window including:

- change the name of the *Home* tab by clicking the name.
- select the number of columns for the page by selecting the *Edit Page Preferences* icon next to the page name.
- add more pages by selecting the *Add page* tab. Additional page tabs will appear at the top of the page window.

To add content, select *Add Content*.

Figure 141: Adding web portal content



A number of content options are available. Select a tab on the left to view the widgets available. To add a particular widget, either double-click to add the content, or select a widget and select *OK*. Holding the Control or Shift keys enables you to select multiple widgets.

Widgets available for the web portal include:

- Application Control List
- Calendar
- Clock
- Installation
- Run Report
- RSS Feed
- Notification
- Text Messages
- Firewall Policies
- Active Directory List
- User List
- URL Category List
- URL Filter List
- Local URL Category List
- Local URL Category Rating List

Once you have selected the widgets, you can move them on the page within the column chosen column view.

You can change the width of the columns. When you move your cursor between the widgets, you will see a line appear, demarcing the column borders. Click and drag left or right to expand or contract the column width.

Many of the widgets are configurable. In the title bar of the widgets, if there is an *Edit* or *Dependencies* icon on the right, further configuration can be done with the widget.

You can resize the widgets vertical size by clicking and dragging the bottom of the widget

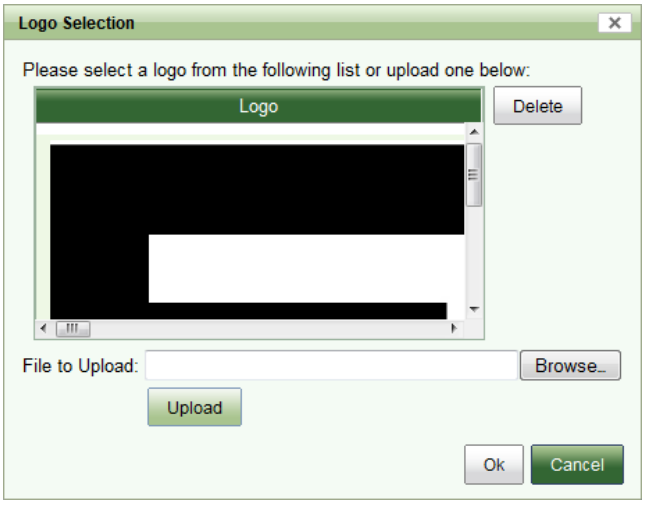
Adding a logo

You can add a logo to the web portal page. The logo can be your logo, or the logo of the user as a part of the customization to go with the color selection. The logo must be a bitmap image. It can be any size, color or monochrome. The logo file can be .jpg, .png, .bmp or .gif. Remember if the logo is too large or detailed, it may take longer for the portal page to load.

To add a logo to the web portal display:

1. Select *Logo Preferences*.

Figure 142: Logo Preferences



2. Select *Browse* and locate the logo on your hard disk or network volume.
3. Select *Upload*.
4. Select the uploaded logo and select *OK*.

Portal Preferences

You can change the colors of the display from a list of color themes. To change the colors of the web portal display, select *Portal Preferences*, select the desired color scheme from the list, and select *OK*.

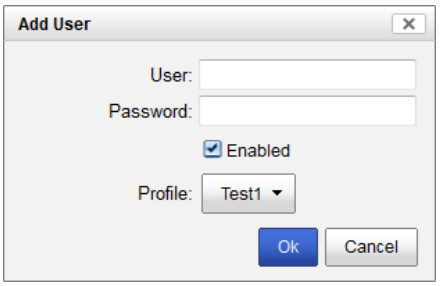
Figure 143: Portal properties window

Creating a portal user account

To create a portal user account, go to *Device Manager* > *Tools* > *Web Portal*, select the *Portal Users* tab, and select *Add User*. The *Add User* dialog opens. Enter or select the following items and select *OK*.

The user name can be up to 35 characters and the password up to 20 characters.

Figure 144: Add User window



User	Enter the name of the user who will log into the portal.
Password	Enter the password for the user.
Enabled	Select to enable the user profile.
Profile	Select the profile for this user from the list.

External users

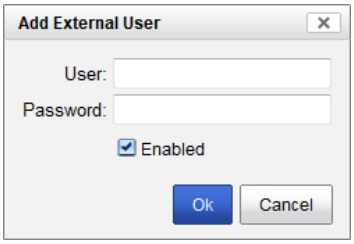
Use the *External Users* tab to add external users. This enables users to have remote access to the managing FortiManager unit from the portal FortiManager unit.

You also use external users when creating custom widgets that you can add on custom portal web pages or web portals such as iGoogle.

To add external users:

1. Go to *Device Manager* > *Tools* > *Web Portal* and select the *External Users* tab.
2. Select *Add External User*.
3. Enter the required information and select *OK*.

Figure 145: Add External User window



User	Enter a name for the external user.
Password	Enter a password for the external user.
Enabled	Select to enable the external user.

Using the web portal

The purpose of the web portal is to enable customers, or their administrators the ability to monitor and maintain their firewall settings.

Before the users can use the web portal you need to supply them with the following information:

- the URL or IP address of the FortiManager system
- the user name
- the user password

The user enters the FortiManager system URL or IP address into the web browser. When they get the login screen, they enter the supplied user name and password. This will log them into the portal site, displaying the colors, widgets and arrangements setup from the previous steps.

The administrator can view firewall information, maintain and update information depending on the widgets included for the portal. The user can log out of the portal by selecting the *Logout* button in the upper right corner of the browser window.

Application Program Interfaces

FortiManager has two application program interfaces (APIs): an Extensible Markup Language (XML) based API for automation and to facilitate integration, and the web portal SDK for creating administrative web portals for clients.

This chapter includes:

- XML API
- Fortinet developer network

XML API

FortiManager includes a Web Services interface to facilitate integration with provisioning systems and automate the configuration of the many devices that FortiManager is capable of managing. The FortiManager API is XML-based. You can use the XML API to obtain information from the FortiManager unit, create and run FortiOS CLI scripts to modify device configurations, and install the modified configurations on your managed devices.

Connecting to FortiManager web services

To start working with web services on your FortiManager unit, enable web services and obtain the Web Services Description Language (WSDL) file that defines the XML requests you can make and the responses that FortiManager can provide.

Enabling web services

You must enable web services on the network interfaces to which Web Services clients will connect.

To enable web services on an interface using the Web-based Manager:

1. Go to *System Settings* > *Network*.
2. If you want to enable Web Services for all interfaces, select *Web Service* in the *Administrative Access* section.
3. If you want to enable Web Services for a specific interface:
   - Select the *All Interfaces* button.
   - Select the name of the interface that you want to use.
   - In the *Administrative Access* section, select *Web Service*.
4. Select *OK*.

To enable web services on an interface using the CLI:

1. Enter the following CLI commands:

```
config fmsystem interface
  edit <port>
    set allowaccess webservice
  end
```

   where `<port>` is the network interface that you want to use for web services.

   The `allowaccess` command should also include the other types of administrative access that you want to permit. For example, to allow HTTPS, SSH, and Web Services, enter the command `set allowaccess https ssh webservice`.

The FortiManager unit handles web services requests on port 8080.

Obtaining the WSDL file

You can download the WDSL file directly from the URL https://<ip_address>:8080/.

You can also use the Web-based Manager to download the WSDL file. Go to *System Settings* > *Advanced* > *Advanced Settings* and select the *Download WSDL file* icon.

By using a web testing tool such as SoapUI, you can get information from the FortiManager.

Fortinet developer network

The Fortinet developer network is designed for multi-tenancy applications within a single management platform. This feature is a Javascript Object Notation (JSON) based application program interface (API) that allows managed security service providers (MSSPs) to offer administrative web portals to their customers. It provides an administrative web portal for customers who require some degree of control over their network security environment.

Fortinet developer network requires a separate license. To purchase a license, contact your Fortinet partner or reseller.

Java-based Administration Client

This section provides general information about the java-based administration client, a web user interface for accessing the system from a client computer.

This section includes the following topics:

- System requirements
- Installing and logging in to the Java-based client
- Java-based manager overview
- Java-based manager features

System requirements

The management computer that is used to access the java-based manager must have Java installed on a compatible operating system.

Installing and logging in to the Java-based client

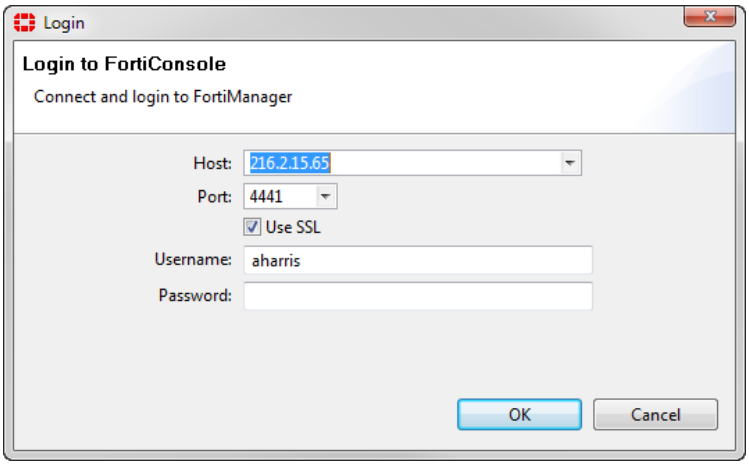
Java must be installed prior to attempting to install the Java-based administration client.

To install the java-based administration client:

1. Connect to the Web-based Manager. See "Connecting to the Web-based Manager" on page 32.
2. Click on the *Download FortiConsole* button in the menu bar.
3. Select *Open With... Java Web Start Launcher*.

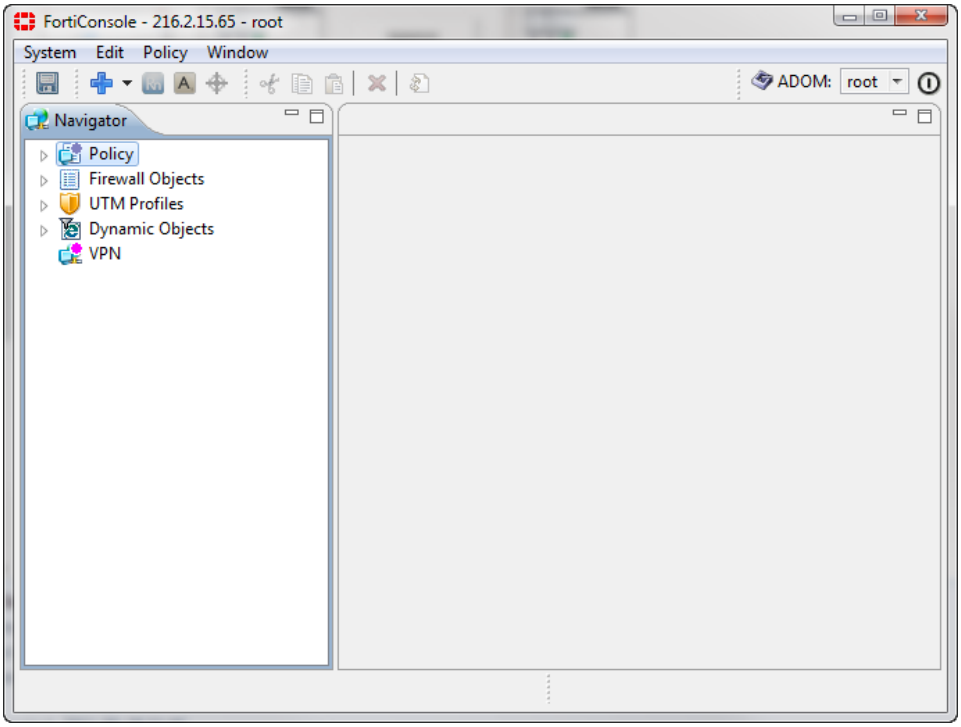
   The java-based client is installed and opens to the login screen.

Figure 146: Java-based administration client login screen



4. Enter the required information on the login screen and click *Login*.
   The Java-based manager main window opens.

Figure 147: Java-based administration client main window



Only one person can login to the system with read/write privileges at a time. If a user is already logged in, you can either login as read-only, or automatically force the other user to log out.

Java-based manager overview

The Java-based administration client provides many of the same functions as the Web-based Manager (see "Using the Web-based Manager" on page 32). The Java-based manager is a desktop application and thus has faster performance than the Web-based Manager.

The three primary parts of the FortiManager java-based interface are the Main Menu Bar, the navigation pane, and the content pane. The option also exists to include a Console Pane, which shows all the data sent to and received from the server.

All of the panes are tab based. For more information see "Tabs" on page 211.

The Java-based manager cannot be used to add devices to the FortiManager system.

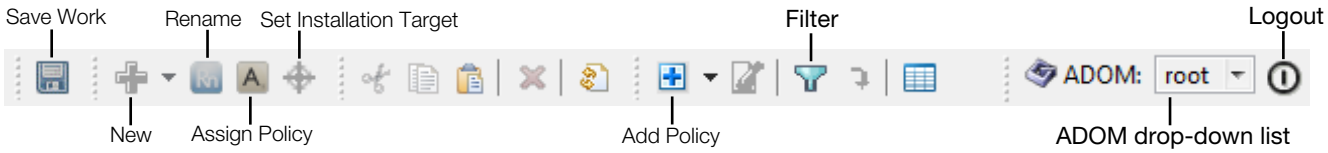
This section describes the following topics:

- Using the main toolbar
- Using the navigation pane
- Using the content pane

Using the main toolbar

By default, the main menu bar is displayed at the top of the manager window. It can be moved to any location on the window by clicking and dragging the menu bar.

Figure 148: Default main menu bar



The menu bar is dynamic; the available icons on the bar change depending on the current selection. The important icons available are:

Save work	Select to save any changes that have been made to the system using the Java-based manager.
New	Select to create a new policy package or folder.
Rename	Select to rename the selected policy or folder.
Assign Policy	
Set Installation Target	Select to set the devices or groups that the selected policy is to be installed on within the selected ADOM.
Add Policy	Select to add a new policy for the ADOM.
Filter	Select to filter the information in the content pane based on the contents of the available columns.
ADOM	Select an ADOM to manage from the drop down list. Select *Global* to manage all ADOMs.
Log Out	Select to log out of the FortiManager Web-based Manager.

Using the navigation pane

The Java-based manager navigation pane is, by default, located down the left sidebar of the window. It provides access to the Policy, Firewall Objects, UTM Profiles, Dynamic Objects, and VPN elements of the selected ADOM.

Folders can be created in the navigation pane. Policies can then be moved into the folders to improve the organization of the tree without affecting the functionality of any of the elements.

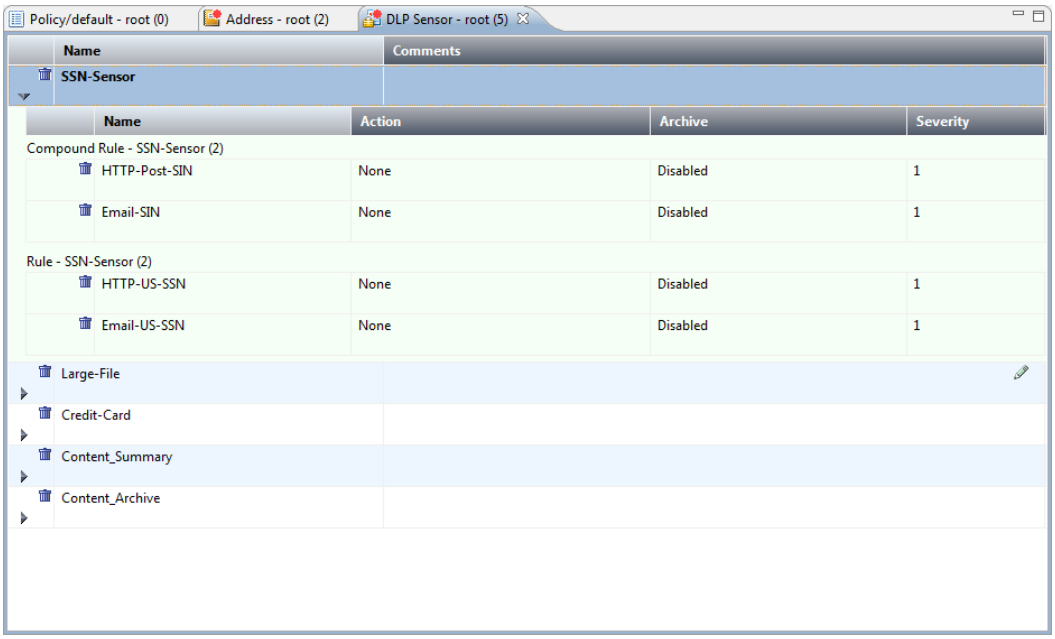
For more information see “Device Management” on page 135.

Using the content pane

The content pane displays information about the selected element in the navigation pane. Multiple tabs can be opened to show information from multiple elements. See “Tabs” on page 211 for more information.

The elements can be edited and rules can be added in different ways depending on the selected element. See “Device Management” on page 135 for more information.

Figure 149: Java-based manager content pane



Right-clicking on the column headings will open a pop-up menu with options for configuring how the information is displayed in the columns, including what columns are displayed, and the optional of adding new rows to the table.

To change the data in a row, right-click on the far left cell of the row and select edit from the pop-up menu. Some information can be changed by simply double-clicking on the cell itself and then editing the cell information.

Certain row elements can be changed from drop-down lists. These elements will have a small arrow in the lower-right corner of the cell that can be clicked on to open the drop-down list.

If applicable, children rows can be added to a row. This can be done by either clicking on the arrow in the lower left-hand corner of the first cell in the row, or in a sub-window in the row editing window.

Java-based manager features

The Java-based administration client contains features not available in the Web-based Manager.

Drag and drop

The Java-based administration client a drag and drop feature that simplifies adding and editing object information.

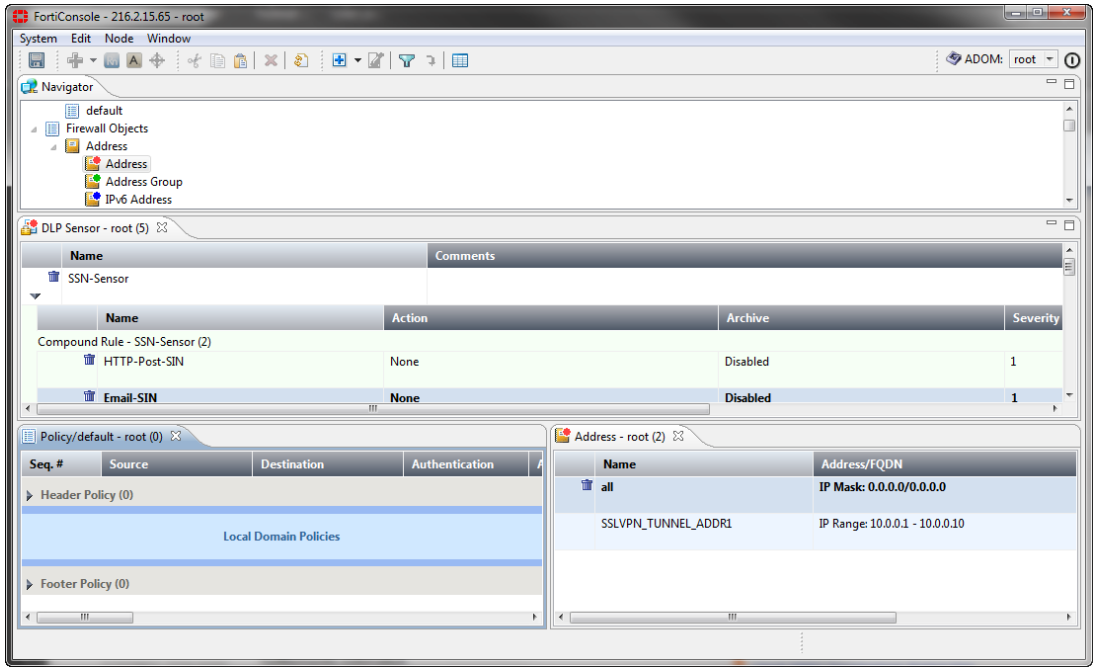
Data, such as member names, can be dragged from the Data Source window and dropped into the requisite location on the add/edit window. For options where there is a long list of data, a search function can be used, allowing the data to be filtered based on given criteria.

Tabs

All of the panes in the Java-based administration client are tab based. Multiple tabs can be opened in any pane, allowing for multiple nodes (such as policies or objects) to be edited simultaneously and for nodes to be compared side by side. Tabs can also be removed from panes and left floating on the screen.

Figure 150 shows the tabs reorganized into a horizontal configuration.

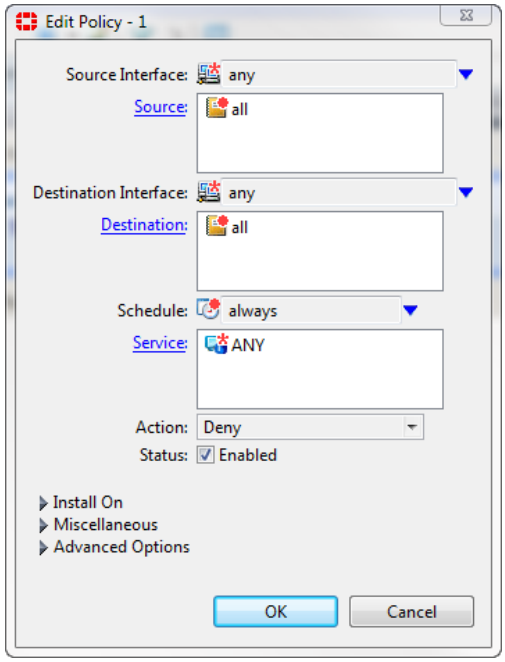
Figure 150: Reorganizing tabs in the Java-based administration client



Improved adding and editing windows

The adding and editing windows are redesigned in the Java-based manager to improve functionality and usability. In conjunction with the "Drag and drop" feature, adding and editing policies and objects is faster and easier with the Java-based manager.

Figure 151: Policy editor widow



Working with Scripts

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

Any scripts that are run on the global database must use complete commands. For example, if the full command is *config system global*, do not use *conf sys glob*.

Scripts can be written in one of two formats. The first format contains a sequence of FortiGate CLI commands, as you would type them at the command line. A comment line starts with the number sign (#). A comment line will not be executed.

The second format uses TCL scripting commands to provide more functionality to your scripts including global variables and decision structures.

When writing your scripts, it is generally easier to write them in a context-sensitive editor, and then cut and paste them into the script editor on your FortiManager system. This can help avoid syntax errors and can easily reduce the troubleshooting required for your scripts.

This section contains the following topics:

- Device view
- Script samples

For information about scripting commands, see FortiGate CLI reference.

Before using scripts, ensure the `console more` function has been disabled in the FortiGate CLI. Otherwise scripts and other output longer than a screen in length will not execute or display correctly.

Device view

While in *Device Manager*, select a FortiGate device and select *System* > *Script Status*. This is the script status page for that device, or the default script view. This page shows all the scripts loaded into the device and also shows schedules for executing them and script execution history.

This is different from the Script Repository where all the scripts on your FortiManager system are listed, not just scripts for one device or group. Go to *Device Manager* > *Script* to view scripts available for all devices. For more information, see “Script view” on page 216.

Individual device view

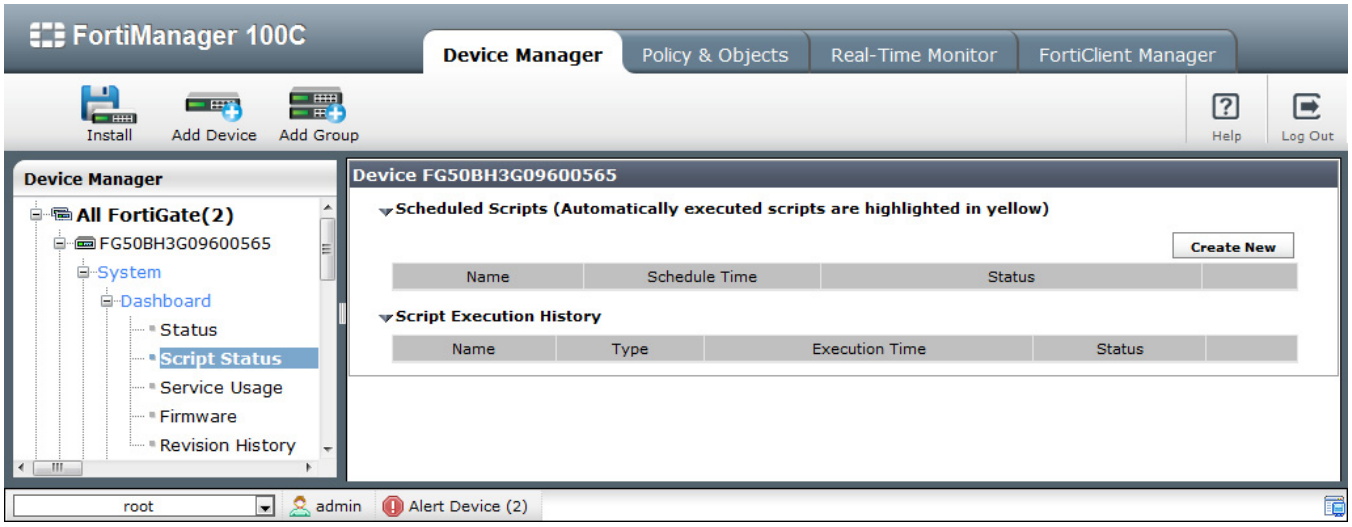
From the initial *Device Manager* view, of an individual device, selecting the *System* > *Dashboard* > *Script Status* brings you to the script view for that device.

From the initial *Device Manager* view, of a device group, selecting the *<group_name>* > *Script* brings you to the script view for that device group.

The name of the device or device group is displayed at the top of the screen. This view has two sections: scheduled scripts, and script execution history.

To create a new schedule to execute a script, see "To schedule a script:" on page 215.

Figure 152: Individual device view



The following information and options are available

Scheduled Scripts	Select the arrow to expand or collapse this section. For more information on scheduling scripts, see "Scheduling a script" on page 215.
Create New	Select to schedule the execution of a script on this device. For more information on scheduling scripts, see "Scheduling a script" on page 215.
Name	The name of the script that has been scheduled to execute on this device.
Schedule Time	The date and time this script is scheduled to execute. If it is a recurring schedule, additional information such as the day of the week is displayed here. Based on the type of script schedule, the following information is displayed: • One-time - date and time the script will execute • Recurring daily- time the script will execute. • Recurring weekly - weekday and time the script will execute • Recurring monthly - day of the month and time the script will execute • Automatic - this row has a yellow background, but no text is displayed. The script will only execute when the configuration on the device or group is installed.

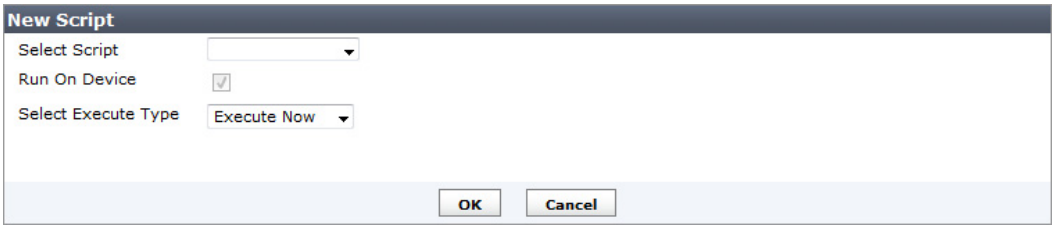
Status	The type of schedule for this script - either Scheduled or Automatic. Scheduled can be one of one-time, recurring daily or recurring monthly.
Edit icon	Select to modify the schedule for the script. You can change it to *Execute Now*, *Scheduled* or *Automatic* as well as changing the schedule information.
Delete icon	Select to cancel the scheduled script.
Script Execution History	Select the arrow to expand or collapse this section.
Name	The name of the script that was executed on this device.
Type	Specifies whether the script was executed on the local FortiManager database or on the device or device group.
Execution time	The date and time when the script ran.
Status	The status of the script execution. Status is *Done* if the script executed correctly and *Error* if the script encountered an error and couldn't finish.
Browse icon	Select to view the Script History. This is the output that was displayed during the execution of the script and will include error information if an error has occurred.

Scheduling a script

From the individual or group device views, you can select *Create New* to schedule one or more existing scripts to execute on that device or group.

Scheduling a script on a group of devices is the same as for a single device, except that you can exclude devices from the group. These excluded devices will not execute this scheduled script.

Figure 153: Scheduling a script



To schedule a script:

1. Go to D*evice Manager*, select the device and select *System* > *Script Status*.

   For a device group, select the device group and select *Script*.
2. Select *Create New*.
3. Select a script from the *Select Script* list. If there are no scripts in this list, create a new script. For more information, see "Creating or editing a script" on page 218.
4. Select *Run On DB (Only CLI Scripts)* to have your script run on the FortiManager device database instead of directly on the managed device. This option is not available for TCL scripts.

5. Select the Execute Type as one of:
   - Execute now - runs the script on the device when you select OK.
   - Schedule - displays additional options for selecting the type of scheduling, date, and time.
   - Automatic - the script will execute when the configuration on this device or group is committed or deployed.
6. Select scheduling information as required.
   - For a *One-Time* schedule, select the calendar icon to browse calendar months to quickly select the month and day of the month.
   - For a *Recurring* schedule, select the type as one of daily, weekly or monthly. For weekly, select the day of the week to run the script. For monthly, select the day of the month to run the script. Select the hour and minute to run the script on that day. Hours are based on the 24-hour clock.
7. For a group of devices, optionally select which devices in the group to exclude.
8. Select *OK* to save this script schedule, and return to the device or group view.

Script view

You can use the *Device Manager* script repository to add, clone, edit, delete, and export scripts. You can also execute CLI scripts on the global database and view the results of running the script.

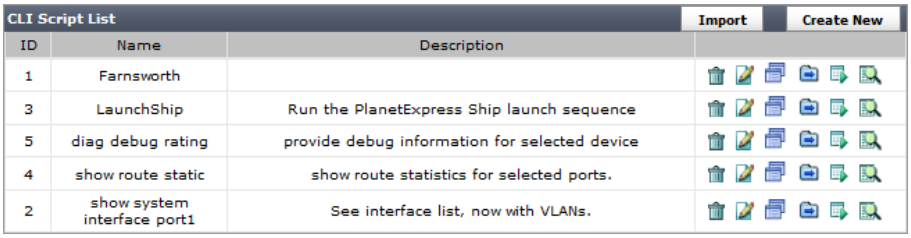
To view the list of scripts, go to *Device Manager* > *Tools* > *Script*.

The tools menu will only be visible if *Show Device Manager Tools* has been enabled in the administrator settings. See “Configuring global admin settings” on page 93.

You can select *CLI Script, CLI Script Group*, or *TCL Script*. CLI scripts only allow you to use Fortinet CLI commands in your script. TCL scripts allow you to use TCL scripting language commands which can include CLI commands as well. CLI Script Group is grouping some scripts together that will be run, making it easier to schedule multiple scripts at one time.

When you are creating, editing, or deleting scripts you are working in the Script Repository.

Figure 154:CLI script repository



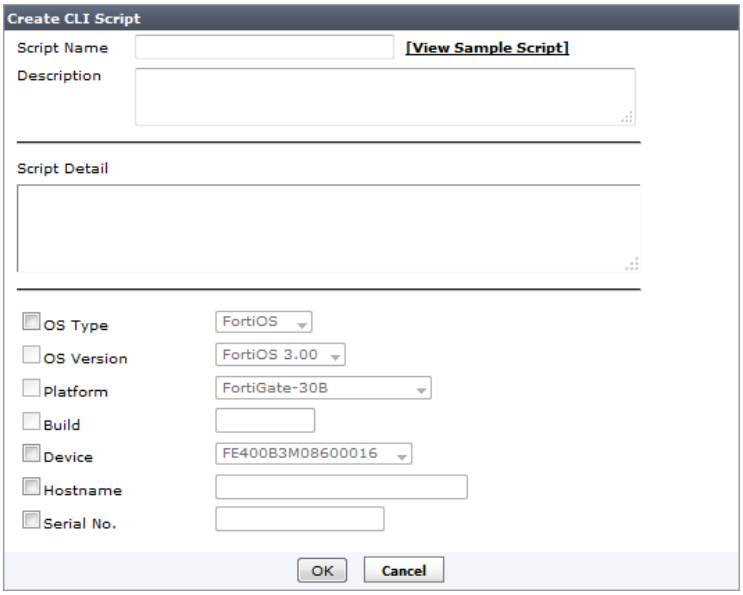
The following information and options are available:

Import	Select to import a script. The script will be imported from a plain text file on your local computer.
Create New	Select to create a new script. For more information, see “Creating or editing a script” on page 218.
ID	The ID assigned to this script.
Name	The name of the script. The script name can include spaces, but cannot include punctuation.
Description	A brief description of the script.
Delete icon	Select this icon to delete this script. If this icon does not appear, the script is in use and cannot be deleted at this time. Generally this indicates the script has been scheduled to run on a device at a later date.
Edit icon	Select to view or change the script information.
Clone icon	Select to create a duplicate of this script with another name. For more information, see “Cloning a script” on page 219.
Export icon	Export a script in the form of a text file that you can download to your PC. The default name of the file is script.txt.
Run script now icon	Select to run this script on the FortiManager global database. Only CLI scripts can be run on the global database, and the CLI commands must be the full command, no short forms.
View Log icon	Select to view the log of this script running on the global database. Select *Return* to come back to this screen when done.

Creating or editing a script

From the *Device Manager* script screen, you can create a new script or edit an existing script.

Figure 155: Create or edit a script



To create or edit a script:

1. Go to *Device Manager* > *Tools* > *Script* and select either *CLI Script* or *TCL Script*.
2. Select either *Create New* or select the *Edit* icon for the script to edit.
3. If you are creating a script, enter a short descriptive name for this script. The name should be unique and easy to recognize. If you are editing an existing script, the script name is read-only.

   For tips and examples on how to write scripts, select the *View Sample Script* link to open a small online help window that contains various script examples.
4. Enter a description of what action(s) the script performs. As with the script name, keep the description short and useful.
5. Enter your script in the *Script Detail* field by:
   - entering the commands manually (for CLI or TCL scripts)
   - cutting and pasting from a FortiGate unit CLI (for CLI scripts)
   - cutting and pasting from an editor of your choice (for CLI or TCL scripts)

   For information on writing CLI or TCL scripts, see “Script samples” on page 220.

When creating a script, use full command syntax instead of abbreviations.

For longer TCL scripts, a context sensitive editor is recommended to reduce errors.

TCL scripts cannot include the TCL exit command.

6. Optionally you can add information to limit what devices can run the script. This includes selecting the OS Type, OS Version, platform, firmware build, device name, hostname of the device, and serial number.
7. Select *OK* to save your new script and return to the Script Repository.

After creating or editing a script, you can test it using the script procedure in “Scheduling a script” on page 215. If your script does not execute properly, see “Script samples” on page 220 for troubleshooting tips.

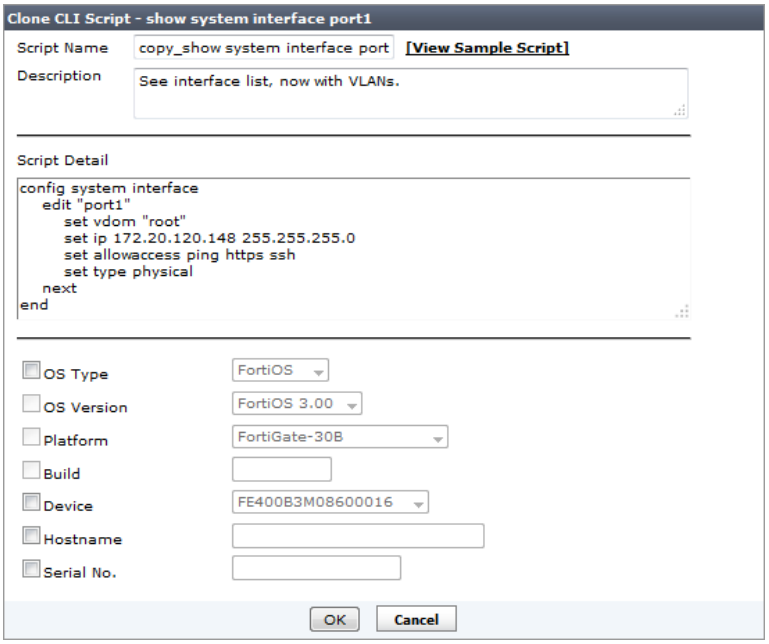
Cloning a script

Cloning is a fast way to create a new script that shares some commands with an existing script. It can avoid typos and be easier than cutting and pasting.

To clone a script:

1. Go to *Device Manager* > *Script*, select either *CLI Script* or *TCL Script*, and select the *Clone* icon for the script you want to duplicate.

Figure 156: Cloning a script



2. Enter a new name for the duplicate script.

   By default it is given the same name as the original script with the prefix of “copy_”, so a script called “test” would result in a default duplicate called “copy_test”.
3. Optionally enter a new description.

   It is recommended to change the description when cloning. This is another method to ensure the original the cloned scripts are not confused for each other.
4. Edit the script to make the necessary changes.
5. Save your new script.

Exporting a script

You can export scripts as text files.

To export a script:

1. Go to *Device Manager* > *Script*, select either *CLI Script* or *TCL Script*, and select the *Export* icon for the script you want to export.
2. Download the text file to your PC.

Script samples

This section helps familiarize you with FortiManager scripts, provides some script samples, and provides some troubleshooting tips.

The scripts presented in this section are in an easy to read format that includes:

- the purpose or title of the script
- the script itself
- the output from the script (blank lines are removed from some output)
- any variations that may be useful
- which versions of FortiOS this script will execute on

Do not include `\r` in your scripts as this will cause the script to not process properly.

Script samples includes:

- CLI scripts
- TCL scripts

CLI scripts

CLI scripts include only FortiOS CLI commands as they are entered at the command line prompt on a FortiGate device. CLI scripts do not include TCL commands, and the first line of the script is not “#!” as it is for TCL scripts.

CLI scripts are useful for specific tasks such as configuring a routing table, adding new firewall policies, or getting system information. These example tasks easily apply to any or all FortiGate devices connected to the FortiManager system.

However, the more complex a CLI script becomes the less it can be used with all FortiGate devices - it quickly becomes tied to one particular device or configuration. One example of this is any script that includes the specific IP address of a FortiGate device’s interfaces can not be executed on a different FortiGate device.

Samples of CLI scripts have been included to help get you started writing your own scripts for your network administration tasks.

Error messages will help you determine the causes of any CLI scripting problems, and fix them. For more information, see “Error Messages” on page 224.

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 224.

CLI script samples

There are two types of CLI scripts. The first type is getting information from your FortiGate device. The second type is changing information on your FortiGate device.

Getting information remotely is one of the main purposes of your FortiManager system, and CLI scripts allow you to access any information on your FortiGate devices. Getting information typically involves only one line of script as the following scripts show.

To view interface information for port1:	
Script	show system interface port1

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

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

To view the entries in the static routing table:	
Script	show route static

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

Variations	none

To view information about all the configured FDN servers on this device:

Script

```
diag debug rating
```

Output

```
Locale       : english

The service is not enabled.
```

Variations

Output for this script will vary based on the state of the FortiGate device. The above output is for a FortiGate device that has never been registered.

For a registered FortiGate device without a valid license, the output would be similar to:

Locale : english

License : Unknown

Expiration : N/A

Hostname : guard.fortinet.net

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

IP Weight Round-time TZ Packets Curr Lost Total Lost

** None **

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

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

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

Script

```
config system accprofile
   edit "policy_admin"
      set avgrp read
      set fwgrp read
      set ipsgrp read
      set loggrp read
      set spamgrp read
      set sysgrp read
      set webgrp read
   next
end
```

Output	Starting script execution config system accprofile (accprofile)# edit "policy_admin" set avgrp read set fwgrp read set ipsgrp read set loggrp read set spamgrp read set sysgrp read set webgrp read next end exit new entry 'policy_admin' added (policy_admin)# set avgrp read (policy_admin)# set fwgrp read (policy_admin)# set ipsgrp read (policy_admin)# set loggrp read (policy_admin)# set spamgrp read (policy_admin)# set sysgrp read (policy_admin)# set webgrp read (policy_admin)# next (accprofile)# end MyFortiGate # MyFortiGate # MyFortiGate # exit
Variations	This profile is read-only to allow a policy administrator to monitor this device's configuration and traffic. Variations may include enabling other areas as read-only or write privileges based on that account type's needs.

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

- Running a CLI script on a FortiGate unit

```
config firewall policy
  edit 1
    set srcintf “port1”
    set dstintf “port2”
    set srcaddr “all”
    set dstaddr “all”
    set status disable
    set schedule "always"
    set service "ANY"
    set logtraffic enable
    set status enable
```

```
  next
end
```

- Running a CLI script on the global database

```
config firewall policy
  edit 1
    set _global-srcintf "port1"
    set _global-dstintf "port2"
    set srcaddr "all"
    set dstaddr "all"
    set status disable
    set schedule "always"
    set service "ANY"
    set logtraffic enable
    set status enable
  next
end
```

Error Messages

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

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

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

Troubleshooting Tips

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

- Check the script output. Generally the error messages displayed here will help you locate and fix the problem.
- See the *FortiGate CLI Reference* for more information on all CLI commands.
- There is a limit to the number of scripts allowed on the FortiManager unit. Try removing an old script before trying to save your current one.
- As mentioned at the start of this chapter, ensure the `console more` command is disabled on the FortiGate devices where scripts execute. Otherwise a condition may occur where both the FortiGate device and the FortiManager system are waiting for each other to respond until they timeout.
- There should be no punctuation at the start or end of the lines.
- Only whitespace is allowed on the same line as the command. This is useful in lining up `end` and `next` commands for quick and easy debugging of the script.

- Keep your scripts short. They are easier to troubleshoot and it gives you more flexibility. You can easily execute a number of scripts after each other.
- Use full command names. For example instead of “set host test” use “set hostname test”. This is required for any scripts that are to be run on the global database.
- Use the number sign (#) to comment out a line you suspect contains an error.

TCL scripts

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

Do not include the exit command that normally ends TCL scripts; it will cause the script to not run.

This guide assumes you are familiar with the TCL language and regular expressions, and instead focuses on how to use CLI commands in your TCL scripts. Where you require more information about TCL commands than this guide contains, please refer to resources such as the TCL newsgroup, TCL reference books, and the official TCL web site at http://www.tcl.tk.

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

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

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

- TCL variables
- TCL loops
- TCL decisions
- TCL file IO

Limitations of FortiManager TCL

FortiManager TCL executes in a controlled environment. You do not have to know the location of the TCL interpreter or environment variables to execute your scripts. This also means some of the commands normally found in TCL are not used in FortiManager TCL. For more information on the limitations of FortiManager TCL, see your Release Notes, and the Knowledge Base.

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.

To save system status information in an array:

Script

```
#!
proc get_sys_status aname {
  upvar $aname a
  set input [exec "get system status\n" "# "]
  set linelist [split $input \n]
  foreach line $linelist {
    if {![regexp {([^:]+):(.*)} $line dummy key value]} continue
    switch -regexp -- $key {
      Version {
        regexp {Fortigate-([^ ]+) ([^,]+),build([\d]+),.*} $value dummy
a(platform) a(version) a(build)
      }
      Serial-Number {
        set a(serial-number) [string trim $value]
      }
      Hostname {
        set a(hostname) [string trim $value]
      }     }
  }
}

get_sys_status status

puts  "This machine is a $status(platform) platform."
puts  "It is running version $status(version) of FortiOS."
puts  "The firmware is build# $status(build)."
puts  "S/N: $status(serial-number)"
puts  "This machine is called $status(hostname)"

```

Output	`Starting script execution`
	
	`This machine is a 100A platform.`
	`It is running version 4.0 of FortiOS.`
	`The firmware is build# 482.`
	`S/N: FGT100A220120181`
	`This machine is called techdocs-100A.`

Variations	Once the information is in the variable array, you can use it as part of commands you send to the FortiGate device or to make decisions based on the information. For example:
	if {$status(version) == 4.0} {
	# follow the version 4.0 commands
	} elseif {$status(version) == 4.0} {
	# follow the version 4.0 commands
	}

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

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

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

In analyzing this script:

- line 1 is the required #! to indicate this is a TCL script
- lines 2-3 open the procedure declaration
- lines 4-5 puts the output from the CLI command into a TCL variable as a string, and breaks it up at each return character into an array of smaller strings
- line 6 starts a loop to go through the array of strings
- line 7 loops if the array element is punctuation or continues if its text
- line 8 takes the output of line 7's 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.

To create 10 users from usr0001 to usr0010:

Script

```
1  #!
2  proc do_cmd {cmd} {
3  puts [exec "$cmd\n" "# " 15]
4  }
5  set num_users 10

6  do_cmd "config user local"
7  for {set i 1} {$i <= $num_users} {incr i} {
8  set name [format "usr%04d" $i]
9  puts "Adding user: $name"
10 do_cmd "edit $name"
11 do_cmd "set status enable"
12 do_cmd "set type password"
13 do_cmd "next"
14 }
15 do_cmd "end"

16 do_cmd "show user local"

17
```

Output

```
Starting script execution
config user local
(local)#
Adding user: usr0001
edit usr0001
new entry 'usr0001' added
(usr0001)#
set status enable
(usr0001)#
set type password
(usr0001)#
next

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

Fortigate-50A #
show user local

config user local
    edit "usr0001"
        set type password
    next
    edit "usr0002"
        set type password
    next
end

Fortigate-50A #
```

Variations

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

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

In analyzing this script:

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

TCL decisions

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

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

To add information to existing firewall policies:

Script

```
1  #!
2  # need to define procedure do_cmd
3  # the second parameter of exec should be "# "
4  # If split one command to multiple lines use "\" to continue
5
6
   proc do_cmd {cmd} {
7    puts [exec "$cmd\n" "# "]
   }
8  foreach line [split [exec "show firewall policy\n" "# "] \n] {
     if {[regexp {edit[ ]+([0-9]+)} $line match policyid]} {
9      continue
10   } elseif {[regexp {set[ ]+(\w+)[ ]+(.*)\r} $line match key value]} {
11     lappend fw_policy($policyid) "$key $value"
12   }
   }
   do_cmd "config firewall policy"
13 foreach policyid [array names fw_policy] {
14   if {[lsearch $fw_policy($policyid){diffservcode_forward 000011}] == -1} {
15     do_cmd "edit $policyid"
       do_cmd "set diffserv-forward enable"
       do_cmd "set diffservcode-forward 000011"
16     do_cmd "next"
17   }
18 }
   do_cmd "end"
```

Output	
Variations	This type of script is useful for updating long lists of records. For example if FortiOS version 4.0 MR1 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

To get and display state information about the FortiGate device:

Script

```
1  #!
2  #Run on FortiOS v4.00
3  #This script will display FortiGate's CPU states,
4  #Memory states, and Up time
5
6  set input [exec "get system status\n" "# "]
7  regexp {Version: *([^ ]+) ([^,]+),build([0-9]+),[0
8  -9]+} $input dummy status(Platform) status(Version)
9  status(Build)
10
11 if {$status(Version) eq "4.00"} {
12   puts -nonewline [exec "get system performance
13 status\n" "# " 30]
14 } else {
15   puts -nonewline [exec "get system performance\n" "#
16 " 30]
17 }
18
```

Output

```
Starting script execution

get system performance

CPU states:    92% used, 8% idle
Memory states: 55% used
Up:            9 days,  5 hours,  1 minutes.
Fortigate-50B #
```

Variations none.

Versions 4.0

To configure common global settings:

Script

```
1  #!
2
3  #Run on FortiOS v4.00
4  #This script will configure common global settings
5  #if you do not want to set a parameter, comment the
6  #corresponding set command
7  #if you want to reset a parameter to it's default
8  #value, set it an empty string
9
10 set sys_global(ntpserver) "2.2.2.2"
11 set sys_global(admintimeout) ""
12 set sys_global(authtimeout) 20
13 set sys_global(ntpsync) "enable"
14
15 #procedure to execute FortiGate command
16 proc fgt_cmd cmd {
17   puts -nonewline [exec "$cmd\n" "# " 30]
18 }
20 #config system global---begin
21
22 fgt_cmd "config system global"
23 foreach key [array names sys_global] {
24   if {$sys_global($key) ne ""} {
25     fgt_cmd "set $key $sys_global($key)"
26   } else {
27     fgt_cmd "unset $key"
28   }
29 }
30 fgt_cmd "end"
31
32 #config system global---end
33
```

Output

```
Starting script execution
```

Variations none

To configure syslogd settings and filters:

Script

```
#!

#Run on FortiOS v4.00
#This script will configure log syslogd setting and
#filter

#key-value pairs for 'config log syslogd setting', no
#value means default value.
set setting_list {{status enable} {csv enable}
{facility alert} {port} {server 1.1.1.2}}

#key-value pairs for 'config log syslogd filter', no
#value means default value.
set filter_list {{attack enable} {email enable} {im
enable} {severity} {traffic enable} {virus disable}
{web enable}}

#set the number of syslogd server, "", "2" or "3"
set syslogd_no "2"

#procedure to execute 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 log syslogd$syslogd_no setting"
set_kv $setting_list
fgt_cmd "end"

#configure log syslogd setting---end
#configure log syslogd filter---begin
fgt_cmd "config log syslogd$syslogd_no filter"
set_kv $filter_list
fgt_cmd "end"
#configure log syslogd filter---end
```

Output	Starting script execution config log syslogd2 setting (setting)# set status enable (setting)# set csv enable (setting)# set facility alert (setting)# unset port (setting)# set server 1.1.1.2 (setting)# end FGT# config log syslogd2 filter (filter)# set attack enable (filter)# set email enable (filter)# set im enable (filter)# unset severity (filter)# set traffic enable (filter)# set virus disable (filter)# set web enable (filter)# end FGT#
Variations	none

To configure the FortiGate device to communicate with a FortiAnalyzer unit:

Script

```
#!
#This script will configure the FortiGate device to
#communicate with a FortiAnalyzer unit
#Enter the following key-value pairs for 'config
#system fortianalyzer'

set status enable
set address-mode static
set encrypt enable
#localid will be set as the hostname automatically
#later
set psksecret "123456"
set server 1.1.1.1
set ver-1 disable

#for fortianalyzer, fortianalyzer2 or
#fortianalyzer3, enter the corresponding value "",
#"2", "3"
set faz_no ""

#keys used for 'config system fortianalyzer', if you
#do not want to change the value of a key, do not put
#it in the list
set key_list {status address-mode encrypt localid
psksecret server ver-1}

#procedure to get system status from a FortiGate
proc get_sys_status aname {
  upvar $aname a
  set input [split [exec "get system status\n" "# "]
\n]
  foreach line $input {
    if {![regexp {([^:]+):(.*)} $line dummy key
value]} continue
    set a([string trim $key]) [string trim $value]
  }
}#procedure to execute FortiGate command
proc fgt_cmd cmd {
 puts -nonewline [exec "$cmd\n" "# "]
}#set the localid as the FortiGate's hostname
get_sys_status sys_status
set localid $sys_status(Hostname)

#config system fortianalyzer---begin
fgt_cmd "config system fortianalyzer$faz_no"

foreach key $key_list {
 if [info exists $key] {
   fgt_cmd "set $key [set $key]"
 } else {
   fgt_cmd "unset $key"
 } }
fgt_cmd "end"
#config system fortianalyzer---end
```

Output	Starting script execution config system fortianalyzer (fortianalyzer)# set status enable (fortianalyzer)# set address-mode static (fortianalyzer)# set encrypt enable (fortianalyzer)# set localid bob_the_great (fortianalyzer)# set psksecret 123456 (fortianalyzer)# set server 1.1.1.1 (fortianalyzer)# set ver-1 disable (fortianalyzer)# end FGT#
Variations	none

To create custom IPS signatures and add them to a custom group:

Script

```
#!
#Run on FortiOS v4.00
#This script will create custom ips signatures and
#add them to a custom signature group

#Enter custom ips signatures, signature names are the
#names of array elements
set custom_sig(c1) {"F-SBID(--protocol icmp;
--icmp_type 10; )"}
set custom_sig(c2) {"F-SBID(--protocol icmp;
--icmp_type 0; )"}

#Enter custom ips group settings
set custom_rule(c1) {{status enable} {action drop}
{log enable} {log-packet} {severity high}}

set custom_rule(c2) {{status enable} {action reset}
{log} {log-packet disable} {severity low}}

#procedure to execute FortiGate command
proc fgt_cmd cmd {
  puts -nonewline [exec "$cmd\n" "# "]
}

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

Output	Starting script execution config ips custom (custom)# edit c1 new entry 'c1' added (c1)# set signature "F-SBID(--protocol icmp; --icmp_type 10;)" (c1)# next (custom)# edit c2 new entry 'c2' added (c2)# set signature "F-SBID(--protocol icmp; --icmp_type 0;)" (c2)# next (custom)# end FGT# config ips group custom (custom)# config rule c1 (c1)# set status enable (c1)# set action drop (c1)# set log enable (c1)# unset log-packet (c1)# set severity high (c1)# end (custom)# config rule c2 (c2)# set status enable (c2)# set action reset (c2)# unset log (c2)# set log-packet disable (c2)# set severity low (c2)# end (custom)# end FGT #
Variations	none

TCL file IO

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

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

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

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

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

To write to a file:	
Script	1 #! 2 3 set somefile {open “tcl_test” “w”} 4 puts $somefile "Hello, world!" 5 close $somefile 6
Output	
Variations	
Versions	4.0

To read from a file	

Script	1 #!
	2
	3 set otherfile {open “tcl_test” “r”}
	4 while {[gets $otherfile line] >= 0} {
	5 puts [string length $line]
	}
	7 close $otherfile
	8

Output	`Hello, world!`
Variations	

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

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

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

Both scripts close the file before they exit.

Troubleshooting Tips

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

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

FortiGuard Services

The FortiGuard Distribution Network (FDN) provides FortiGuard services for your FortiManager system and its managed devices and 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 intrusion protection engines and signatures
- Web filtering and email filtering rating databases and lookups (select systems)

To view and configure these services, go to *System Settings* > *FortiGuard Center* > *Configuration*. In FortiGuard Center, you can configure the FortiManager system to act as 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 lookup replies to your private network's FortiGate devices and FortiClient agents. The local FDS provides a faster connection, reducing Internet connection load and time required to apply frequent updates, such as antivirus signatures, to many devices. For example, you might enable FortiGuard services to FortiClient agents on the built-in FDS, then specify the FortiManager system's IP address as the override server on your FortiClient agents. Instead of burdening your Internet connection with all FortiClient agents downloading antivirus updates separately, the FortiManager system would use the Internet connection once to download the FortiClient antivirus package update, then redistribute the package to the FortiClient agents.

FortiGuard Center also includes firmware revision management. To view and configure firmware options, go to *System Settings* > *FortiGuard Center* > *Firmware Images*. You can download these images from the Customer Service & Support site to install on your managed devices or on the FortiManager system. For more information, see

Before you can use your FortiManager system as a local FDS, you must:

- Register your devices with 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 and FortiClient agents to the device list, or change the option to allow services to unregistered devices.

  For information about FDN service connection attempt handling or adding devices, see "Viewing FortiGuard services from devices and groups" on page 256 and "Device Management" on page 135. For more information about adding FortiClient agents, see "FortiClient Manager" on page 285.
- Enable and configure the FortiManager system's built-in FDS. For more information, see "Configuring network interfaces" on page 72.
- 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 agents on the device list. For more information, see "Connecting the built-in FDS to the FDN" on page 248.
- Configure each device or FortiClient agent 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 142.

This section contains the following topics:

- FortiGuard center
- Configuring devices to use the built-in FDS
- Configuring FortiGuard services in the FortiGuard Center
- Logging events related to FortiGuard servicesViewing FortiGuard services from devices and groups
- Logging events related to FortiGuard services
- Restoring the URL or antispam database

For information on current security threats, virus and spam sample submission, and FortiGuard service updates available through the FDN, including antivirus, intrusion protection, Web Filtering, and email filtering, see the FortiGuard web site, http://www.fortiguard.com/.

FortiGuard center

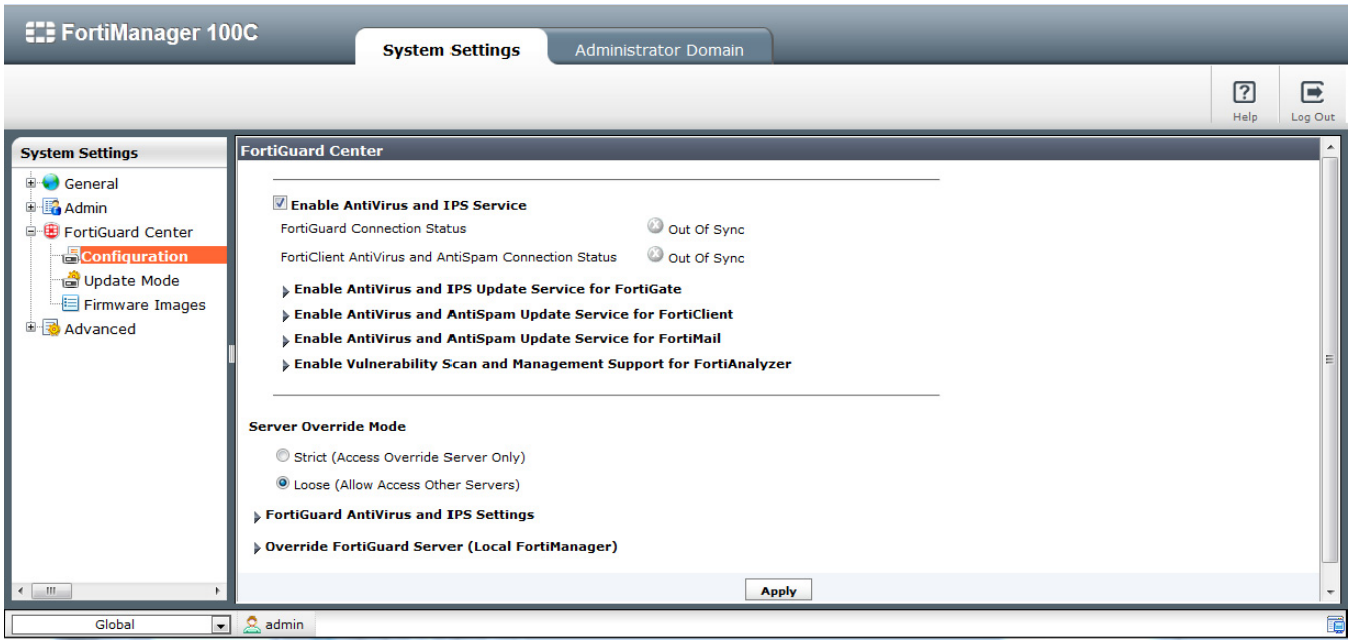
The FortiGuard center, located in *System Settings* > *FortiGuard Center* in the global ADOM, provides a central location for configuring and enabling your FortiManager system's built-in FDS as an FDN override server.

By default, this option is disabled and devices contact FDN directly. After enabling and configuring FortiGuard, and your devices are configured to use the FortiManager system as their FortiGuard server, you can view overall and per device statistics on FortiGuard service benefits. For more information, see "Viewing FortiGuard services from devices and groups" on page 256.

The FortiGuard Center has four supported configuration options:

- Antivirus and IPS Update Service for FortiGate
- Antivirus and Email Filter Update Service for FortiClient
- Antivirus and Email Filter update Service for FortiMail
- Vulnerability Scan and Management Support for FortiAnalyzer

Figure 157: Enable FortiGuard settings



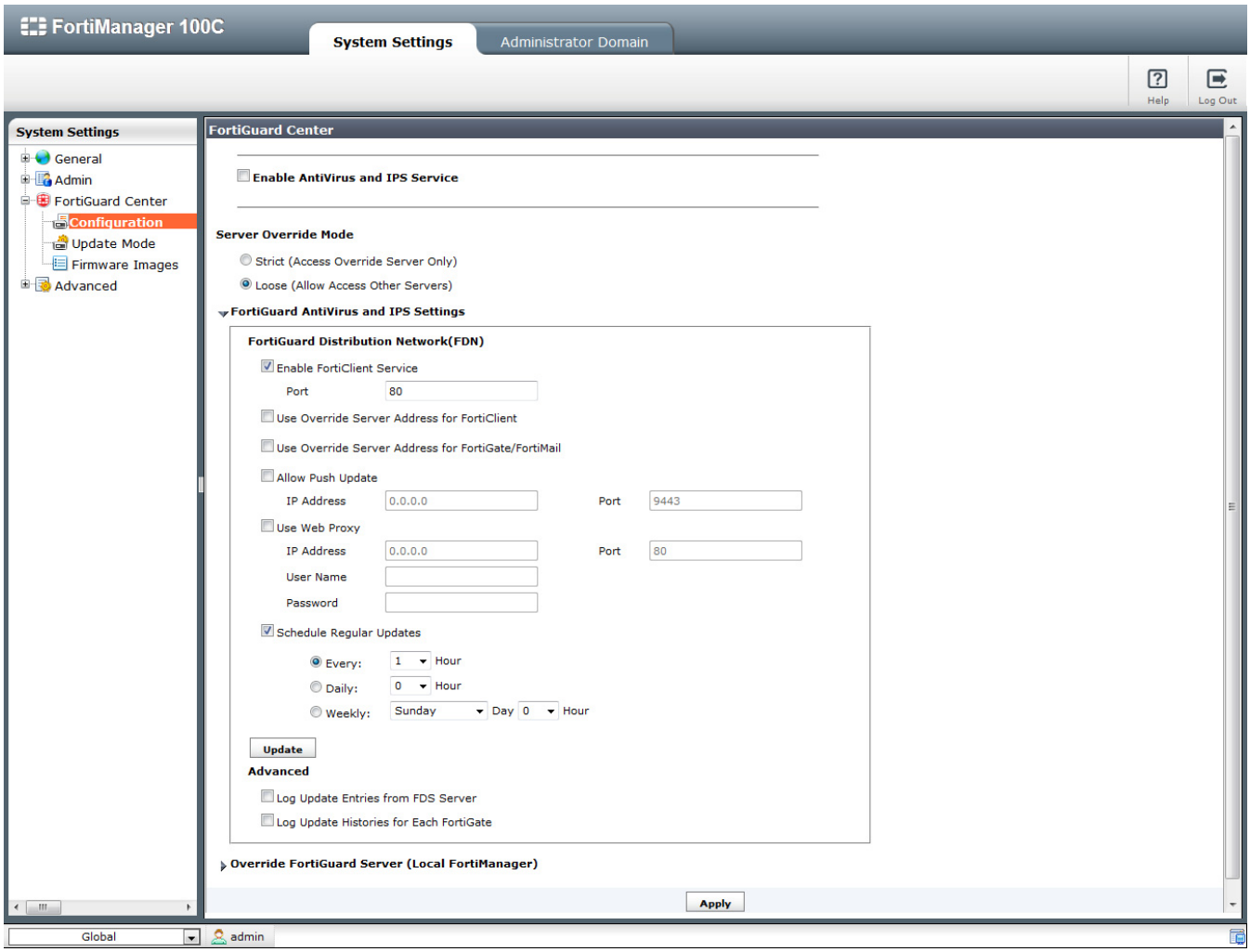
The following information and options are available:

Enable Antivirus and IPS Service	When you select the check box beside *Enable Antivirus and IPS Service*, you are enabling FortiGuard Antivirus and intrusion protection services for FortiGate units. You will also be able to view the status of the AV and (IPS connection for FortiClient.
FortiGuard Connection Status	The status of the current connection between the FDN and the FortiManager system. • **Disconnected** – A red down arrow appears when the FDN connection fails. • **Connected** – A green up arrow appears when the initial FDN connection succeeds, but a synchronization connection has not yet occurred. • **Out of Sync** – A gray X appears when the initial FDN connection succeeds, but the built-in FDS is disabled. • **Synchronized** – A green checkmark appears when the built-in FDS is enabled, and the FDN packages download successfully.
FortiClient Antivirus and Email Filter Connection Status	The status of the current connection to the FDN for FortiClient antivirus and Email Filtering services.
Enable Antivirus and IPS Update Service for FortiGate	The current versions of engines and databases for AV and IPS services that are available on the FDN for FortiGate devices. You enable service updates by selecting the check boxes beside the OS firmware version number. If a check box is not selected, no databases or engines appear, only the OS firmware version number.

Enable Antivirus and Email Filter Update Service for FortiClient	The current versions of engines and databases for antivirus and email filtering services that are available on the FDS for the selected devices. You enable service updates by selecting the check boxes beside the OS firmware version number. If a check box is not selected, no databases or engines appear, only the OS firmware version number.
Enable Antivirus and Email Filter Update Service for FortiMail	The current versions of engines and databases for antivirus and email filtering services that are available on the FDS for the selected devices. You enable service updates by selecting the check boxes beside the OS firmware version number. If a check box is not selected, no databases or engines appear, only the OS firmware version number.
Enable Vulnerability Scan and Management Support for FortiAnalyzer	The current versions of engines and databases for antivirus and email filtering services that are available on the FDS for the selected devices. You enable service updates by selecting the check boxes beside the OS firmware version number. If a check box is not selected, no databases or engines appear, only the OS firmware version number.
Enable Web Filter and Email Filter Service	Select to enable the service.
FortiGuard Web Filter and Email Filter Connection Status	The status of the current connection between the FDN and the FortiManager system. • **Disconnected** – A red down arrow appears when the FDN connection fails. • **Connected** – A green up arrow appears when the initial FDN connection succeeds, but a synchronization connection has not yet occurred. • **Out of Sync** – A gray X appears when the initial FDN connection succeeds, but the built-in FDS is disabled. **Synchronized** – A green checkmark appears when the built-in FDS is enabled, and the FDN packages download successfully.
Server Override Mode	Select the server override mode as either *Strict* or *Loose*.
FortiGuard Antivirus and IPS Settings	See “FortiGuard Antivirus and IPS settings” on page 246.
Override FortiGuard Server (Local FortiManager)	Configure and enable alternate FortiManager FDS devices, rather than using the local (current) FortiManager system. You can set up as many alternate FDS locations, and select what services are used. To configure access to public Web Filtering and email filtering servers, see “Accessing public FortiGuard web filtering and email filtering servers” on page 253

FortiGuard Antivirus and IPS settings

Figure 158: FortiGuard Antivirus and IPS Settings



The following information and options are available:

Enable FortiClient Service	Configure AV and IPS settings for FortiClients. Select to enable and if applicable, enter the port number that will be receiving FortiGuard service updates for FortiClient.
Use Override Server Address for FortiClient	Configure to override the default built-in FDS so that you can use a port or specific FDN server. To override the default server for updating FortiClient's FortiGuard services, see "Overriding default IP addresses and ports" on page 252.
Allow Push Update	Configure to allow urgent or critical updates to be pushed directly to the FortiManager system when they become available on the FDN. The FortiManager system immediately downloads these updates. To enable push updates, see "Enabling updates through a web proxy" on page 251.

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 251.
Scheduled Regular Updates	Configure when packages are updated without manually initiating an update request. To schedule regular service updates, see "Scheduling updates" on page 252.
Update	Select to immediately update the configured antivirus and email filtering settings.
Advanced	Enables logging of service updates and entries. If either check box is not selected, you will not be able to view these entries and events when you select View FDS and FortiGuard Download History.

FortiGuard web filter and email filter settings

Connection to FDS server(s)	Configure connections for overriding the default built-in FDS or web proxy server for web filter and email filtering settings. To override an FDS server for web filtering and email filtering services, see "Overriding default IP addresses and ports" on page 252. To enable web filtering and email filtering service updates using a web proxy server, see "Enabling updates through a web proxy" on page 251.
Log Settings	Configure logging of FortiGuard Web Filtering and email filtering events or configure access to • To configure logging of FortiGuard Web Filtering and email filtering events, see "Logging FortiGuard Web Filtering or Email Filter events" on page 261
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. To configure access to public Web Filtering and email filtering servers, see "Accessing public FortiGuard web filtering and email filtering servers" on page 253
View FDS and FortiGuard Download History	View the types of FortiGuard services that occurred, such as poll and push updates, from FDS, FortiGuard or FortiClient.
Additional number of private FortiGuard servers (excluding this one) (1) +	Select the + icon to add a private FortiGuard server. When adding a private server, you must enter its IP address and time zone. Private FortiGuard servers are used for

Enable Antivirus and IPS Update Service for Private Server	When one or more private FortiGuard servers are configured, update AV 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 filtering and email filtering 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 72.

Connecting the built-in FDS to the FDN

When you enable the built-in FDS, and initiate an update either manually or by schedule, the FortiManager system attempts to connect to the FDN.

If all connection attempts to the server list fail, the connection status will be Disconnected.

If the connection status remains Disconnected, you may need to configure the FortiManager system's connection to the FDN by:

- overriding the default IP address and/or port
- configuring a connection through a web proxy

After establishing a connection with the FDN, the built-in FDS can receive FortiGuard service update packages, such as antivirus engines and signatures or Web Filtering database updates, from the FDN.

To enable the built-in FDS:

1. Go to *System Settings* > *FortiGuard Center* > *Configuration*.
2. Enable the types of FDN services that you want to provide through your FortiManager system's built-in FDS.

   For more information, see "Configuring FortiGuard services in the FortiGuard Center" on page 250.

3. Select *Apply*.

   The built-in FDS attempts to connect to the FDN. To see the connection status go to *System Settings* > *FortiGuard Center* > *Configuration*.

Disconnected	A red down arrow appears when the FDN connection fails.
Connected	A green up arrow appears when the initial FDN connection succeeds, but a synchronization connection has not yet occurred.
Out Of Sync	A gray X appears when the initial FDN connection succeeds, but the built-in FDS is disabled, and so cannot synchronize.
Synchronized	A green checkmark appears when the built-in FDS is enabled, and FDN package downloads were successfully completed.

If the built-in FDS cannot connect, you may also need to enable the selected services on a network interface. For more information, see "Configuring network interfaces" on page 72.

If you still cannot connect to the FDN, check routability, DNS, and any intermediary firewalls or NAT devices for policies that block necessary FDN ports and protocols. For additional FDN troubleshooting information, including FDN server selection, "FDN port numbers and protocols" on page 252 and the Knowledge Base article FortiGuard Distribution Network: Accessing and Debugging FortiGuard Services.

Configuring devices to use the built-in FDS

After enabling and configuring the FortiManager system's built-in FDS, you can configure devices to use the built-in FDS by providing the FortiManager system's IP address and configured port as their override server.

Devices are not required to be registered with FortiManager system's *Device Manager* to use the built-in FDS for FortiGuard updates and services. For more information, see "Viewing FortiGuard services from devices and groups" on page 256.

Procedures for configuring devices to use the built-in FDS vary by their device type. See the documentation for your device for 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 "Configuring network settings" on page 70.

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 intrusion protection 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 *Unregistered Device Options* is configured to allow connections from unregistered devices, unregistered devices can also connect.

For example, you might choose to manage a FortiGate unit's firmware and configuration locally (from its web-based manager), but use the FortiManager system when the FortiGate unit requests FortiGuard Antivirus and attack updates. In this case, the FortiManager system considers the FortiGate unit to be an unregistered device, and must decide how to handle the connection attempt. The FortiManager system will handle the connection attempt as configured in Unregistered Device Options.

Unregistered FortiClient connections are handled in *FortiClient Manager*.

To configure connection attempt handling:

1. Go to *Device Manager* > *Unregistered Device* > *Unregistered Device Options*.
2. Select which action the FortiManager system performs when receiving a connection attempt from an unregistered device:
   - Add unregistered devices to device table, but ignore service requests

     The device appears in the Unregistered Devices item in the device list, but its connection attempt is otherwise ignored.
   - Add unregistered devices to device table, and allow FortiGuard service and central management service.

     The device appears in the Unregistered Devices item in the device list, and will be allowed to receive FortiGuard services.
3. Select *Apply*.

Configuring FortiGuard services in the FortiGuard Center

The FortiGuard Center provides a central location for configuring how the FortiManager system accesses the FDN and FDS, including push updates. The following procedures explain how to configure FortiGuard services and configuring override and web proxy servers, if applicable.

If you need to host a custom URL list that are rated by the FortiGate unit, you can import a this list using the CLI.

Enabling push updates

When an urgent or critical FortiGuard AV 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 251.

If push updates must occur through a firewall or NAT device, you may also need to override the default push IP address and port.

For example, overriding the push IP address can be useful when the FortiManager system has a private IP address, and push connections to a FortiManager system must traverse NAT. Normally, when push updates are enabled, the FortiManager system sends its IP address to the FDN; this IP address is used by the FDN as the destination for push messages; however, if the FortiManager system is on a private network, this IP address may be a private IP address, which is not routable from the FDN – causing push updates to fail.

To enable push through NAT, enter a push IP address override, replacing the default IP address with an IP address of your choice such as the NAT device's external or virtual IP address. This causes the FDN to send push packets to the override IP address, rather than the FortiManager system's private IP address. The NAT device can then forward the connection to the FortiManager system's private IP address.

The built-in FDS may not receive push updates if the external IP address of any intermediary NAT device is dynamic (such as an IP address from PPPoE or DHCP). When the NAT device's external IP address changes, the FortiManager system's push IP address configuration becomes out-of-date.

To enable push updates to the FortiManager system:

1. Go to *System Settings* > *FortiGuard Center* > *Configuration*.
2. Select the arrow to expand the *FortiGuard Antivirus and IPS Settings*; see Figure 158 on page 246.
3. Select the check box beside *Allow Push Update*.
4. If there is a NAT device or firewall between the FortiManager system and the FDN which denies push packets to the FortiManager system's IP address on UDP port 9443, enter the IP Address and/or Port number on the NAT device which will forward push packets to the FortiManager system. The FortiManager system will notify the FDN to send push updates to this IP address and port number.
   - IP Address is the external or virtual IP address on the NAT device for which you will configure a static NAT or port forwarding.
   - Port is the external port on the NAT device for which you will configure port forwarding.
5. Select *Apply*.
6. If you performed step 4, also configure the device to direct that IP address and/or port to the FortiManager system.
   - If you entered a virtual IP address, configure the virtual IP address and port forwarding, and use static NAT mapping.
   - If you entered a port number, configure port forwarding; the destination port must be UDP port 9443, the FortiManager system's listening port for updates.

Enabling updates through a web proxy

If the FortiManager system's built-in FDS must connect to the FDN through a web (HTTP or HTTPS) proxy, you can specify the IP address and port of the proxy server.

If the proxy requires authentication, you can also specify a user name and password.

To enable updates to the FortiManager system through a proxy:

1. Go to *System Settings* > *FortiGuard Center* > *Configuration*.
2. Expand *FortiGuard Antivirus and IPS Settings*; Figure 158 on page 246.

3. Select the check box beside *Use Web Proxy* and enter the IP address and port number of the proxy.
4. If the proxy requires authentication, enter the user name and password.
5. Select *Apply*.
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.

If the FDN connection status is Disconnected, the FortiManager system cannot connect through the web proxy.

Overriding default IP addresses and ports

FortiManager systems' built-in FDS connect to the FDN servers using default IP addresses and ports. You can override these defaults if you want to use a port or specific FDN server that is different from the default.

To override default IP addresses and ports:

1. Go to *System Settings* > *FortiGuard Center* > *Configuration*.
2. If you want to override the default IP address or port for synchronizing with available FortiGuard Antivirus and Intrusion Protection (IPS) updates, select the arrow to expand *FortiGuard Antivirus and IPS Settings*.
   - Select the check box beside *Use Override Server Address for FortiGate* and enter the IP address and/or port number for all FortiGate units.
   - Select the check box beside *Use Override Server Address for FortiClient* and enter the IP address and/or port number for all FortiClients.
3. Select *Apply*.
4. Select *Update* to immediately connect and receive updates from the FDN.

   The FortiManager system connects to the override server and receives updates from the FDN.

If the FDN connection status remains disconnected, the FortiManager system cannot connect with the configured override.

FDN port numbers and protocols

Both the built-in FDS and devices use certain protocols and ports to successfully request and receive updates from the FDN or override server. Any intermediary proxies or firewalls must allow these protocols and ports, or the connection will fail.

For troubleshooting information and details on FDN ports, see and the Knowledge Base article FDN Services and Ports.

After connecting to the FDS, you can verify connection status on the FortiGuard Center page. For more information about connection status, see "Connecting the built-in FDS to the FDN" on page 248.

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 *System Settings* > *FortiGuard Center* > *Configuration*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*; Figure 158 on page 246.
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:

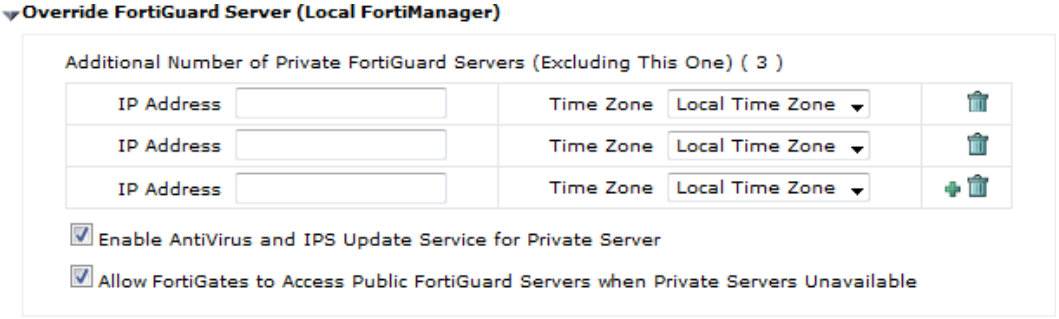
1. Go to *System Settings* > *FortiGuard Center* > *Configuration*.
2. Select the arrow to expand *FortiGuard Web Filter and Email Filter Settings*.
3. In *Polling Frequency*, select the number of hours and minutes of the polling interval.
4. Select *Apply*.

If you have formatted your FortiManager system's hard disk, polling and lookups will fail until you restore the URL and email filtering databases. For more information, see "Restoring the URL or antispam database" on page 263.

Accessing public FortiGuard web filtering and email filtering servers

You can configure the FortiManager system to allow the managed FortiGate units to access public FortiGuard web filtering or email filtering network servers in the event local FortiGuard web filtering or email filtering server URL lookups fail. You can specify up to two private servers (which includes the current one) where the FortiGate units can send URL queries.

Figure 159: Overriding FortiGuard Server



To access public FortiGuard web filter and email filter servers:

1. Go to *System Settings* > *FortiGuard Center* > *Configuration*.
2. Expand *Override FortiGuard Server (Local FortiManager)*.
3. Select the *Plus* sign next to *Additional number of private FortiGuard servers (excluding this one)*.
4. Enter the *IP Address* for the server, and select its *Time Zone*.
5. Repeat step 4 as often as required. You can include up to ten additional servers.
6. Select the additional options to set where the FDS updates come from, and if the managed FortiGate units can access these servers if the local FDS is not available.
   - Check the *Enable Antivirus and IPS update Service for Private Server* if you want the FDS updates to come from a private server.
   - Click *Allow FortiGates to access public FortiGuard servers when private servers unavailable* if you want to the updates to come from public servers in case the private servers are unavailable.
7. Select *Apply*.

Manually uploading AV and IPS updates

The built-in FDS will retrieve AV and IPS update packages from the FDN automatically at the scheduled time, then re-distribute them to requesting devices; however, you can also manually upload the AV and IPS packages to the FortiManager system, and manually re-distribute them to devices.

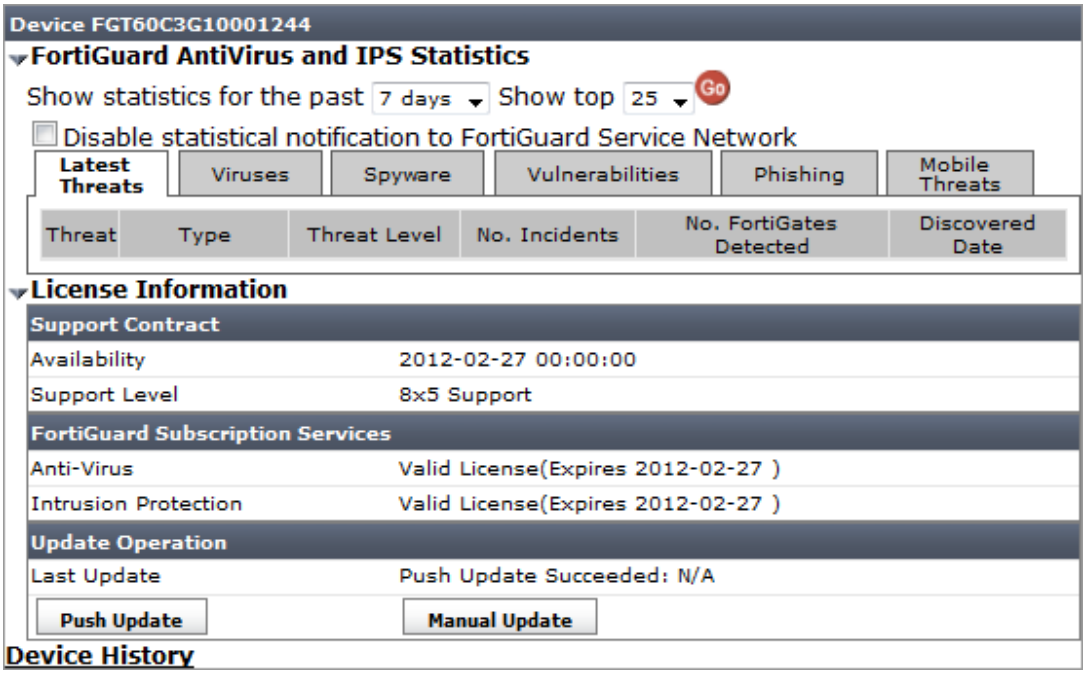
- You can retrieve AV and IPS update packages from the Fortinet Customer Service & Support web site to your computer, then upload them to the FortiManager system. This can be useful if your FortiManager system must distribute packages other than the ones currently available from the FDN. (In this case, you would also disable synchronization with the FDN.)
- You can manually distribute update packages to devices from the FortiManager system. This can be useful when the AV and IPS packages are reverted, which can occur when restoring device firmware.

Uploads to devices can be initiated by either push or traditional upload methods. Both methods require you to enable SSH and HTTPS administrative connections from the FortiManager system's IP address on the device's network interface. Push requires that the device is enabled to receive push messages.

To manually upload AV or IPS updates to one or more devices:

1. Select a device in the device manager.
2. Select *System* > *Dashboard* > *Service Usage*.

Figure 160: Manually uploading AV or IPS updates



3. Select the tab for the type of threat to be manually updated.
4. Scroll to the bottom of the page and select *Manual Update*.
5. Select the antivirus or IPS file to be uploaded and click *Push*.
6. Select *OK*.

   The FortiManager system uploads the selected package to the selected device(s).

To push AV or IPS updates to one or more devices:

1. Select a device in the device manager.
2. Select *System* > *Dashboard* > *Service Usage*; see Figure 160 on page 255
3. In the *License Information* area, select *Push* for the device that you want to update.

   A UDP message announcing the availability of the most current update is sent to the device. If the device is enabled to receive push updates, it then downloads the update from the FortiManager system.

Manual uploads do not bypass the requirement that the FortiManager system must be able to connect to the FDN to validate device licenses for FortiGuard Antivirus and IPS.

Viewing FortiGuard services from devices and groups

The *Device Manager* can be used to display FortiGuard license information and threat detection statistics for devices that use the FortiManager unit for FortiGuard service updates and queries. You can also push or manually issue FortiGuard service updates to devices registered with *Device Manager*.

FortiGuard service statistics for an individual device or group are not available until you:

- enable FortiGuard services via the built-in FDS (see "Connecting the built-in FDS to the FDN" on page 248)
- enable FortiGuard service logging (see "Logging events related to FortiGuard services" on page 260)
- register and connect the device/group to *Device Manager*
- provide the device/group with valid FortiGuard service licenses
- configure the device/group to request FortiGuard updates and ratings from the FortiManager system, instead of the public FDN

Statistic columns are sortable. For example, you could sort device names in ascending order (from A to Z), or IP addresses in descending order (from high to low numbers).

To sort columns in ascending or descending order, select the column heading. Each time you click the column heading, the column will cycle between ascending and descending order. An arrow next to the column heading indicates the current sort order: an up arrow indicates ascending order, and a down arrow indicates descending order. By default, columns are in ascending order.

To view a device's FortiGuard service usage statistics:

1. From the *Device Manager* select a device.
2. Select *System* > *Dashboard* > *Service Usage*; see Figure 160 on page 255

Statistics are not available for unregistered devices. Additionally, the FortiManager system cannot send Manual Update or Push messages to unregistered devices.

To view device group's FortiGuard service usage statistics:

1. From the *Device Manager* select a device group.
2. Select *System* > *Dashboard* > *Service Usage*.

FortiGuard Antivirus and IPS Statistics for a device

If AV and IPS updates from the built-in FDS are currently disabled, a warning message about the service being disabled appears:

To view FortiGuard Antivirus and IPS statistics for a device, in the device manager select a device and select *Relay Service*. Then select the arrow to expand *FortiGuard Antivirus and IPS Statistics*.

Show statistics for the past *n*	Select a number of days (up to 7) to view statistics for that period of time and then select *Go*.
Show top *n*	Select a number to view the top threat types and then select *Go*.

Disable statistical notification to FortiGuard Service Network	Select if you do not want FortiManager system to send statistical information on threats to Fortinet. By default, this feature is enabled.
Latest Threats, Viruses, Spyware, Vulnerabilities, Phishing, Mobile Threats	Select a tab to view detailed information about the latest threats, viruses etc. detected on the selected FortiGate device.
Threat, Virus, spyware, Vulnerability, Phishing, Mobile Threat	The name of the threat, virus etc.
Type	The category of threat, such as a Mass-Mailer.
Threat Level	The severity level of the threat (virus etc.): the higher the severity, the higher the threat level.
%	The threat level as a percent.
No. Incidents	The number of times that the threat was detected.
No. FortiGates Detected	The number of FortiGate devices that detected the threat.
Discovered Date	The date that Fortinet added the ability to recognize the threat, such as an IPS signature, virus signature, etc.

Web filter category detail

Web filter category detail displays FortiGuard web filtering category and rating statistics, and is available on FMG-3000 series and greater.

To view Web Filtering category details for a device, in the device manager select a device and select *Relay Service*. Then select the arrow to expand *Web Filter Category Detail*.

FortiGuard web filter and email filter statistics

Web filtering and email filtering statistics track the number of rating queries and their associated bandwidth, and are available on FMG-3000 series and greater.

Statistics are either a group total, or only for the device, depending on whether you have selected a single device or a group in the navigation pane.

If web filtering and email filtering lookups from the built-in FDS are currently disabled, the following message appears:

```
Warning: This Update Manager service is currently disabled
```

To view FortiGuard web filtering and email filtering statistics for a device, in the device manager select a device and select *Relay Service*. Then select the arrow to expand *FortiGuard Web Filter & Email Filter Statistics*.

License information

License information includes devices' FortiGuard service licenses, support contracts and update status. Statistics are either a group total, or only for the device, depending on whether you have selected a single device or a group in the navigation pane.

Single device license information

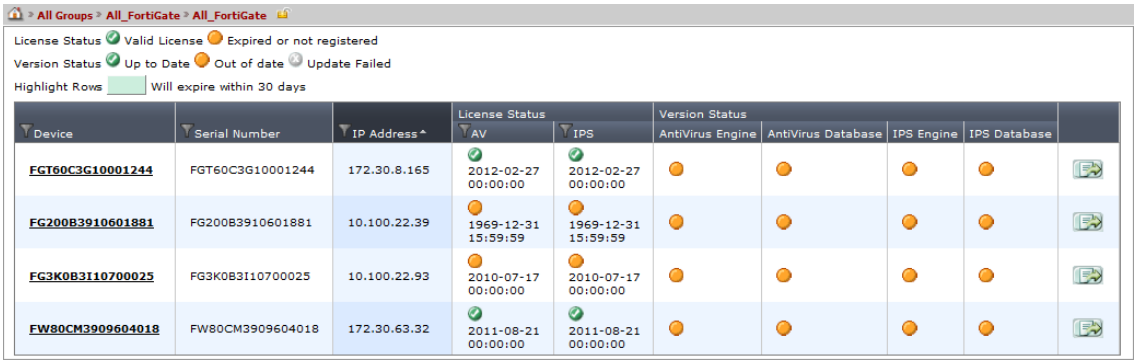
To view license information for a device, in the device manager select a device and select *Relay Service*. Then select the arrow to expand *License Information*.

Support Contract	Information about the device's support contract.
Availability	The date on which the support contract became valid.
Support Level	The level of support that Fortinet provides for the device.
FortiGuard Subscription Services	
Anti-Virus	The status of the FortiGuard subscription for antivirus.
Intrusion Protection	The status of the FortiGuard subscription for Intrusion Protection and application control.
Web Filtering	The status of the FortiGuard subscription for Web Filtering.
Email Filter	The status of the FortiGuard subscription for email filtering.
Update Operation	
Last Update	The last update that was attempted (push update or scheduled update) and whether the update succeeded or failed.
Push Update	If push updates are enabled an configured for the FortiGate device, select Push to send an update availability notification to the FortiGate device. For more information about enabling and configuring push updates, see "Connecting the built-in FDS to the FDN" on page 248.
Manual Update	Select to manually update AV and IPS signatures by selecting antivirus and IPS signature files stored on the FortiManager device and selecting *Push*.

Device group license information

To view license information for a device group, select a device group and select *Service Usage* for that device group.

Figure 161: Device group service usage: license Information



The following information and options are available:

Device, Serial Number, IP address	Identifying information for the devices in the device group. You can sort the information in the table by selecting these column headings.
License Status	Displays the license status for antivirus, intrusion protection, web filtering, and email filtering and firmware manager. The status of each license is displayed using the icons described at the top of the Web-based Manager page: • Valid License: This license is valid and up-to-date. • Expired or not registered: This license is not valid. It is either expired and requires renewing, or has not been registered yet. • Unknown: The status of this license can not be determined. Check the device for more information.
Version Status	Displays the version status for AV engine, AV database, IPS engine, and IPS database. The status of each license can be one of: • Up to date - This version is the most recent available version. • Out of date - This version can be updated to a newer version. • Unknown - This version can not be determined. Check the device for more information.
Push icon	Select to start a push update on this device. A message will be displayed with the device, action taken, and the result.

Device History

Device History (also called Service History) provides historical data on what services have been uploaded successfully to the device.

To view device history for a device, in the device manager select a device and select *System* > *Dashboard* > *Service Usage*. Then scroll to the bottom of the page and select *Device History*.

View *n* **Per Page**	The number of lines you are currently viewing on the page. Select 50, 100, 200 or 500 lines.
Line *n* **/** *n*	The current line you are viewing out of the total number of lines, for example, line 2 of 50. Enter a number to go to a specific line, for example, 5 to view line 5 in the list. Use the arrows to go to the previous page, next page, first page, or last page.
Date	The date the last update occurred. You can display dates in either ascending order or descending order by selecting the Date column heading.
Download	The AV and IPS versions that were downloaded to that device.
AVEN	Whether the AV engine is up to date, out of date, or if the last update failed.
AVDB	Whether the AV database is up to date, out of date, or if the last update failed.
IPSEN	Whether the IPS engine is up to date, out of date, or if the last update failed.
IPSDB	Whether the IPS database is up to date, out of date, or if the last update failed.

Logging events related to FortiGuard services

You can log a variety of events related to FortiGuard services. Depending on your logging selections and which aspect you want to view, you may be able to view these events from these locations:

- from *System Settings* > *Local Log* > *Log Access*
- from *System Settings* > *FortiGuard Center* > *Log* > *Update Log*
- from *System Settings* > *FortiGuard Center* > *Log* > *Download History*

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 AV and IPS updates to both the FortiManager system's built-in FDS and any registered FortiGate devices which use the FortiManager system's FDS.

To log updates and histories to the built-in FDS:

1. Go to *System Settings* > *FortiGuard Center* > *Configuration*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*; see Figure 158 on page 246.
3. Under the *Advanced* heading, enable *Log Update Entries from FDS Server*.

4. Select *Apply*.

To log updates to FortiGate devices:

1. Go to *System Settings* > *FortiGuard Center* > *Configuration*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*; see Figure 158 on page 246.
3. Under the *Advanced* heading, enable *Log Update Histories for Each FortiGate*.
4. Select *Apply*.

Logging FortiGuard Web Filtering 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 filtering events.

To log rating queries:

1. Go to *System Settings* > *FortiGuard Center* > *Configuration*.
2. Select the arrow to expand *FortiGuard Web Filtering and Email Filter Settings*.
3. Select the log settings:

FortiGuard Web Filtering	
Log URL rating misses	Logs URLs without ratings.
Log all URL lookups	Logs all URL lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
FortiGuard Email Filter	
Log all Spam lookups	Logs all spam lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
Log non-spam events	Logs email rated as non-spam.

4. Select *Apply*.

Viewing service update log events

You can view the logged service update events from either the FortiGuard Center or from a device or device group.

To view updates to registered FortiGate devices which use the FortiManager system's FDS, select a device from the device manager, select *Relay Service*, and select *Device History*.

To view update logs for the built-in FDS:

1. Go to *System Settings* > *FortiGuard Center* > *Log* > *Download History*.
2. From the *Service* list, select either *FDS*, *FGD* or *FCT*.
   - FDS: Packages that the FortiManager system can redistribute to FortiGate units, for their local use.
   - FCT: Packages that the FortiManager system can redistribute to FortiClient installations.
   - FGD: Packages that the FortiManager system uses to respond to queries, such as URL rating queries, from FortiGate units.

   Service indicates the category of packages downloaded by the FortiManager system.
3. From the *Event* list, select one of the following: *All Event* to view all events, *Push Update*, *Poll Update*, or *Manual Update*.

   Event indicates the update mechanism, such as updates that occur by either push or poll mechanisms.
4. Select *Go*.

   Details of the selected update events appear:

Date	The date and the time of the update or license check.
Event	The type of the update event, such as Poll Update or Push Update.
Status	The results of the update connection, such as Success, Up to Date, or Connection Failed.
Download	The version number for each item that the built-in FDS can download from the FDN. Download types vary by your selected Service. These appear if Service is FDS:
	• AVEN: FortiGuard Antivirus engine
	• AVDB: FortiGuard Antivirus signature database
	• IPSEN: FortiGuard IPS engine
	• IPSDB: FortiGuard IPS signature database
	• FASE: FortiGuard Antispam engine
	• FASR: FortiGuard Antispam rating
	• FEEN: FortiMail antispam engine
	• FEDB: FortiMail antispam database
	These appear if Service is FGD:
	• SPAM001: FortiGuard Antispam URL database

	• SPAM002: FortiGuard Antispam IP address database
	• SPAM004: FortiGuard Antispam hash database
	• FURL: FortiGuard Web Filtering URL database
	• FGAV: FortiGuard Antivirus query database
	These appear if Service is FCT.
	• FVEN: FortiGuard Antivirus engine for FortiClient
	• FVDB: FortiGuard Antivirus signature database for FortiClient
	• FSEN: FortiGuard Antivirus engine for FortiClient Mobile Symbian
	• FSDB: FortiGuard Antivirus signature database for FortiClient Mobile Symbian
	• FMEN: FortiGuard Antivirus engine for FortiClient Windows Mobile
	• FMDB: FortiGuard Antivirus signature database for FortiClient Windows Mobile
	A green check mark appears next to all version numbers if one or more of the packages was updated during that connection (that is, the Status column is *Success*).
	A gray X appears next to all version numbers if none of the packages were updated during that connection (that is, the Status column is *Up to Date* or *Connection Failed*).

To view update logs from FortiGate devices:

1. Select a device in the device manager.
2. Select *Relay Service*.
3. Select *Device History*.

Restoring the URL or antispam database

Formatting the hard disk or partition on FMG-3000 units and higher deletes the URL and antispam databases required to provide FortiGuard email filtering 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).

Firmware and Revision Control

Instead of upgrading or downgrading each managed device manually, you can change device firmware through your FortiManager unit.

FortiManager units can store and install FortiGate, FortiCarrier and FortiManager firmware images. FortiManager units can receive local copies of firmware images by either downloading these images from the Fortinet Distribution Network (FDN) or by accepting firmware images that you upload from your management computer.

If you are using the FortiManager unit to download firmware images from the FDN, FortiManager units first validate device licenses, including each member of high availability (HA) clusters. The FDN validates support contracts and provides a list of currently available firmware images. For devices with valid support contracts, you can download new firmware images from the FDN, including release notes.

After firmware images have been either downloaded from the FDN or imported to the firmware list, you can either schedule or immediately upgrade/downgrade a device or group's firmware.

Firmware versions and maintenance releases do not always contain the same configuration options and because these options are different, you may need to configure the device or group and resynchronize its configuration after changing a device or group's firmware.

This section contains the following topics:

- Viewing a device or group's firmware
- Downloading firmware images
- Installing firmware images

Viewing a device or group's firmware

You can view a device or group's currently installed firmware, as well as historical changes of firmware images. You can use this information to determine which devices you may want to upgrade.

In *Device Manager*, the Summary tab displays the firmware version number of the currently installed firmware for an individual device or group. The Firmware tab, located after selecting a device, displays detailed firmware information for an individual device or group, including the currently installed firmware image, scheduled firmware changes, and the history of past firmware changes.

When viewing a device or group's firmware information, you can also schedule a future or immediate firmware change, or clear all future scheduled changes. For more information, see "Installing firmware images" on page 269.

Figure 162: Firmware Information (device)

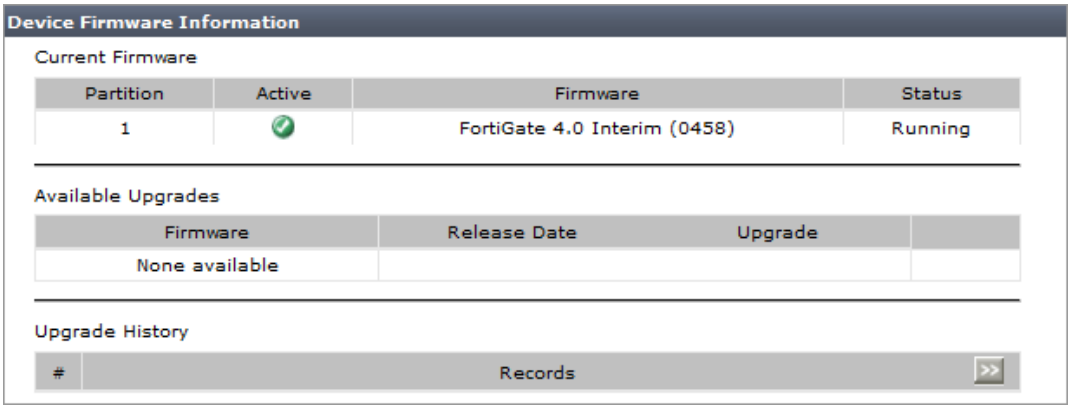


Figure 163: Firmware Information (group)

The following information and options are available:

Schedule Time	The time when the next firmware change is scheduled to begin. Firmware changes can be scheduled at either the individual device or group level.
Image Version	The firmware version that the device will have when the scheduled firmware change is complete.
Status	The upgrade status on the device, such as *None* (if no upgrade is currently scheduled), or *Accepted* (if an upgrade is scheduled, but not yet in progress).
Delete icon	Select to cancel the next scheduled firmware change. This appears only when firmware information displays.
Schedule Upgrade	Select to schedule an immediate or future upgrade for the device.
View History	Select to view a detailed audit trail of all firmware upgrades the device has received from the FortiManager.
Group Members	The firmware version and configuration synchronization information for each device in the group. This does not appear when an individual device is currently selected.
Device	The device's host name.
Model	The device's model.

Firmware	The firmware version currently running on the device.
Status	The configuration synchronization status of the device with the FortiManager unit. If the status is not *Synchronized*, you might need to retrieve or deploy the device's configuration to synchronize the configuration copy stored on the device itself with the local configuration copy stored on the FortiManager unit. For more information about synchronization, see "Checking device configuration status" on page 186.

To view a device or group's firmware details:

1. Go to *Device Manager* and select the type of device you want to view. For example, if you have at least one FortiGate unit registered, *FortiGate* will appear as an option.

   If you want to view a group's firmware details, go to *Device Manager* > *Group*.
2. Select a unit name to view the unit details.

   If want to view the details of a group, select a group name.
3. Select the *Firmware* option from *System* > *Dashboard*.

   The firmware version and any scheduled upgrades for the selected device or group are listed.

If a group is currently selected, collective information is listed, such VDOM status, description, and NAT or transparent operation mode. Information for each device in the group is also listed, so that you can quickly verify devices whose firmware version is different from the group.

To view a device or group's firmware history:

1. Go to *Device Manager* and select the type of device you want to view. For example, if you have at least one FortiGate unit registered, *FortiGate* will appear as an option.

   If you want to view a group's firmware details, go to *Device Manager* > *Group*.
2. Select a unit name to view the unit details.

   If want to view the details of a group, select a group name.
3. Select the *Firmware* option from *System* > *Dashboard*.
4. To view all of a device's firmware history, select the *All History* icon,  , in *Upgrade History.*

   To view all of a group's firmware history, select *View History* and then select *All*.
5. To view a specific time period of a group's firmware history, select *View History*, select *Select*, and then configure the start and end times.
6. Select *OK*.
7. To return to the previous page after viewing either a device or group's firmware history, select *Return*.

   The group or device's firmware version and any scheduled upgrades appear.

If a group is currently selected, collective information is listed, such VDOM status, description, and NAT or transparent operation mode. Information for each device in the group is also listed, so that you can quickly verify devices whose firmware version is different from the group.

To determine if a FortiGate device or group has an available firmware upgrade:

1. Go to *System Settings* > *FortiGuard Center* > *Firmware Images*.
2. Expand a device type to reveal the available firmware versions, maintenance releases and patch releases.
3. Compare the firmware image to the current firmware image on the FortiGate device or group.

You must have root administrative privileges to access *System Settings* > *FortiGuard Center* > *Firmware Images*.

For more information about downloading firmware images, see "Downloading firmware images" on page 267. For information about how to schedule or immediately install a firmware upgrade for a device or group, see "Installing firmware images" on page 269.

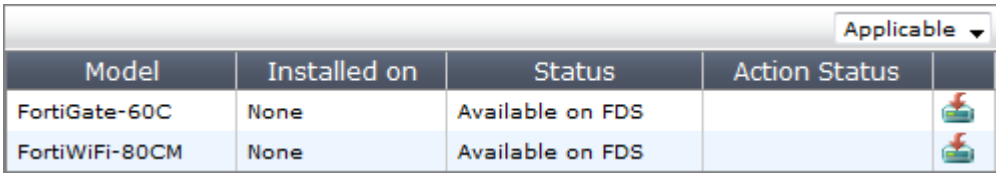
Downloading firmware images

You must first download a local copy of the firmware image to the FortiManager unit to use the FortiManager unit to change managed FortiGate devices' firmware, or to change the FortiManager unit's own firmware.

The Firmware Images page, located in *System Settings* > *FortiGuard Center*, displays all firmware images uploaded to the FortiManager unit from your computer. If a connection to the FDN is available, Firmware Images also displays official FDN releases that you can download to the FortiManager unit. These local copies of firmware images stored on the FortiManager unit are available for use when scheduling firmware changes for FortiGate units, or when changing the firmware of the FortiManager unit itself.

To display all firmware images stored on the FortiManager unit, or to download a local copy of a firmware image, go to *System Settings* > *FortiGuard Center* > *Firmware Images*.

Figure 164: Firmware Images



The following information and options are available:

Base Information	
Release Status	The release status of the firmware image.
Build No.	The build number of the firmware image, which can be used to distinguish different images with the same major release version.
Release Date	The release date of the firmware image.
Release Notes	Select to download the release notes for the firmware image.
Firmware	
Applicable	Select to display only the devices that the specific firmware is for.
All	Select to display all available firmware for all of the devices.
Model	The firmware image's compatible device model.
Installed On	Devices on which the FortiManager unit has installed with that firmware image.
Status	Whether the firmware has been downloaded to the FortiManager unit (*Local*) or is merely available on the FDN (*Available on FDS*).

Action Status	Whether the firmware is pending download (*Accept*) or has completed the download (*Success*).
Delete icon	Delete to local copy of a downloaded firmware image. If a firmware image is deleted, it can be downloaded again.
Download icon	Download a local copy of the firmware image from the FDN. For more information, see "To retrieve an image from the FDN to the FortiManager unit:" on page 268.

To retrieve an image from the FDN to the FortiManager unit:

1. Go to *System Settings* > *FortiGuard Center* > *Firmware Images*.
2. Expand the device type and the firmware version to reveal the available firmware images, and select one of the images.

   If no FDN releases appear in the navigation pane, check the unit's FDN connection.
3. Select *Applicable* if you want to display firmware that is applicable to certain devices. Select *All* if you want to display all available firmware for all devices.
4. In the column corresponding to the device's Model, select *Download*.

If attempts to download the firmware image fail with the error message, "This image is not downloadable," verify that you have registered devices of that model with Customer Service & Support. Images cannot be downloaded unless at least one device of that model has been registered with Fortinet, and has a valid support contract. If these requirements are satisfied, but the error message still appears, wait ten minutes to allow the FortiManager unit to validate device support contracts with the FDN, then retry the download.

To view support contract status and expiration date, in the Device Manager, select the device, then select the *Summary* tab. Support contract information is located in the license information area.

Download time varies by your connection speed and the size of the file. The status and action Status columns indicate if the firmware image is available, if its download to the FortiManager unit is in progress, or if the download has successfully completed.

Table 10: Download progress indicators in Firmware Images

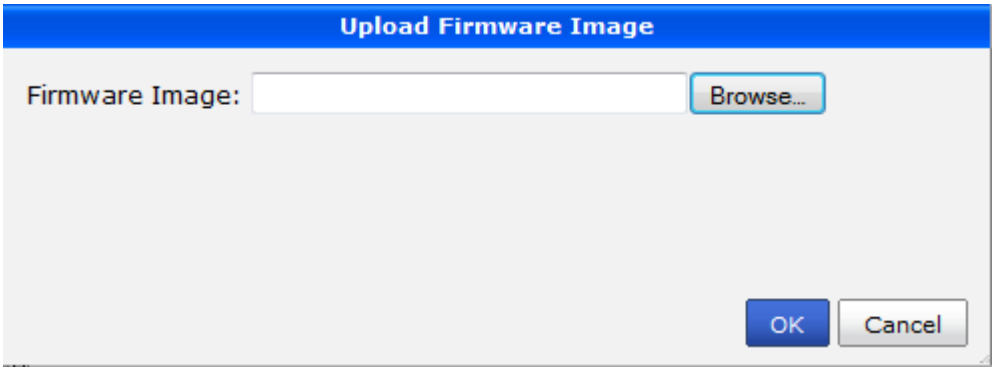
Status	Action Status	Indication
Available on FDS		The firmware image is available on the FDN, but the FortiManager unit has no local copy.
Available on FDS	Accept	The FortiManager unit is currently downloading a local copy of the firmware image.
Local	Success	The FortiManager unit has successfully downloaded a local copy of the firmware image.

To import a firmware image that you have already downloaded to your computer:

1. Go to *System Settings* > *FortiGuard Center* > *Firmware Images* > *Imported*.
2. Select *Create New*.
3. Select *Browse* to locate the file.
4. Select *OK*.

   Upload time varies by your connection speed and the size of the file.

Figure 165: Upload Firmware Image dialog box



To delete a local copy of a firmware image:

1. Go to *System Settings* > *FortiGuard Center* > *Firmware Images* > *Imported*.
2. In the *Imported Firmware Images* list, in the row corresponding to the firmware image that you want to delete, select *Delete*.

   A confirmation message appears.
3. Select *OK*.

Installing firmware images

When you are ready to install a firmware image, use the procedures in "FortiManager Firmware" on page 365. This section provides detailed instructions on how to properly install firmware images to your FortiManager unit and managed devices, including how to test the firmware image before permanently installing it on your FortiManager unit.

You can install firmware images that are either official FDN release images or imported images. When installing a firmware image, you can have the firmware image installed on a specific day and during a specific period of time. For example, you might update firmware during the night when there is less traffic on your network. If you have scheduled a firmware upgrade, you can cancel it.

You cannot cancel firmware changes that:

- have already been attempted at least once, and are configured to retry *n* times
- are currently in progress.

You can immediately change a FortiGate device or group's firmware, or you can schedule a change in the future.

If the FortiManager unit's support contract is invalid or expired, a firmware update can appear to be available from the FDN in *System Settings* > *Firmware Images*. Renew your support contract if, when you select *Download*, a message states that you need to renew the FortiManager unit's support contract.

Real-time Monitor

The Real-Time Monitor (RTM) allows you to monitor your managed devices for trends, outages, or events that require attention. The RTM can be used to monitor any FortiGate, or FortiCarrier device or device group. Where you would normally log on to each individual device to view system resources and information, you can view that same information for all your devices in the RTM.

In the RTM, all actions and configurations are by device. The FortiManager system reads all of its information from the devices via SNMP traps and variables. SNMP traps and variables provide access to a wide array of hardware information from percent of disk usage to an IP address change warning to the number of network connections. SNMP must be properly configured on both the devices and your FortiManager system for this information to be accessible. For more information on SNMP traps, SNMP variables, and FortiManager system SNMP settings, see “Configuring SNMP” on page 98.

The two main parts of RTM are monitoring and alerts. You can use monitoring to view the status information for one or more managed devices. Alerts inform you when an important event occurs on a device, such as a hard disk getting too full. Generally alerts require your attention; in all cases alerts can generate email alerts, log messages or SNMP traps.

To see and change RTM settings, your administrator profile must have RTM enabled. This includes RTM Dashboard, Global, and general RTM settings. For information on administrator profiles, see “Configuring administrator profiles” on page 85.

The following topics are included in this section:

- RTM monitoring
- FortiManager system alerts
- Device log

RTM monitoring

Using RTM monitoring, you can display the RTM dashboard to view the current status of managed devices and monitor alert messages such as device properties or alerts, SNMP traps, and device reachability generated by the devices.

Monitors include:

- Antivirus
- Application Control
- Banned Users
- DHCP
- DLP
- Email Filter
- Endpoint Application
- Endpoint Status
- Endpoint Traffic
- Firewall Policy
- Firewall Session

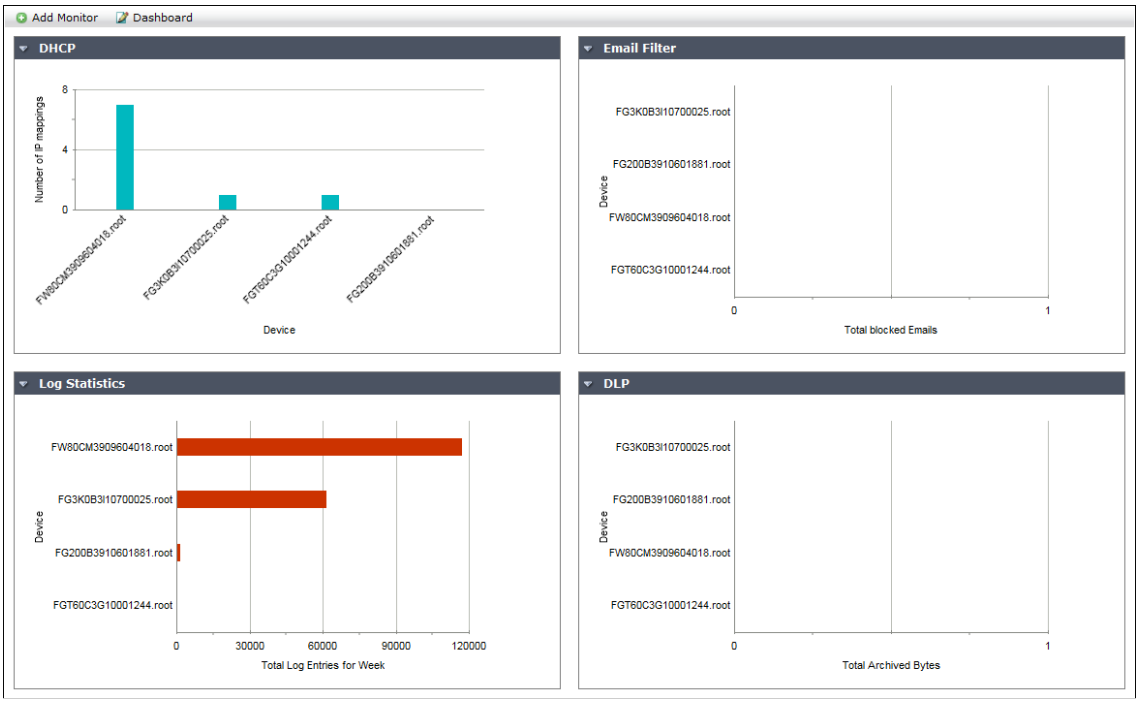
- Firewall Users
- IPsec
- IPv4 Dynamic Routing
- IPv6 Dynamic Routing
- Load Balance
- Log Statistics
- Managed AP
- Modem
- SSL VPN
- Traffic Shaping
- Web Filter
- Wireless Controller
- Wireless Usage

RTM Dashboards

Selecting *Real-Time Monitor* > *Monitoring* > *Dashboard* takes you to the RTM dashboard. RTM dashboards display the current status of managed devices using pre-configured and customizable windows. You can customize RTM dashboards by adding or removing windows and by customizing each window. You can also create multiple dashboards for different kinds of status information and different devices.

When navigating the RTM dashboard, your browser must allow pop-up windows. If not, you will not be able to view many of the configuration screens.

Figure 166: Example RTM Dashboards



The folllowing options are available:

Add Monitor	Add a monitor to the current dashboard.
Dashboards	Select an option from the drop-down list to perform the selected action. For more information, see "Adding and configuring dashboards" on page 272.

Adding and configuring dashboards

To add a new dashboard:

1. Go to *Real-Time Monitor* > *Monitoring* > *Dashboard,* select the *Dashboard* button, and select *Add Dashboard* from the drop-down list.
2. Enter a name for the dashboard.
3. Repeat these steps to create additional dashboards.
4. You can add up to five dashboards.

To delete a dashboard:

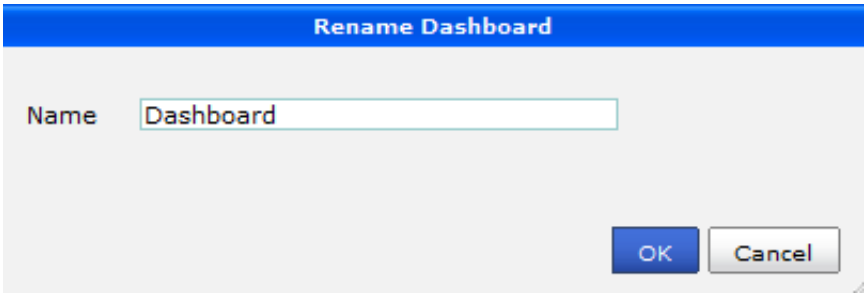
1. Select the dashboard to delete and then select the *Dashboard* button and select *Delete* from the drop-down list.
2. Select *OK* from the pop-up window to confirm the deletion.

   If you hold down the Shift key while deleting a dashboard, the windows on that dashboard are moved the previous dashboard.

To rename a dashboard:

1. Select the dashboard to rename and then select the *Dashboard* button and select *Rename* from the drop-down list.
2. Enter a new name for the dashboard in the *Rename Dashboard* dialog box and select *OK*.

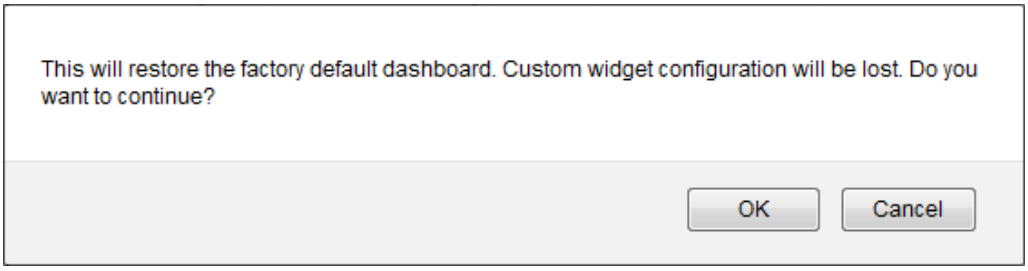
Figure 167: Rename a dashboard



To reset a dashboard:

1. Select the dashboard to rename and then select the *Dashboard* button and select *Reset* from the drop-down list.
2. Select *OK* in the dialog box.

Figure 168: Reset a dashboard

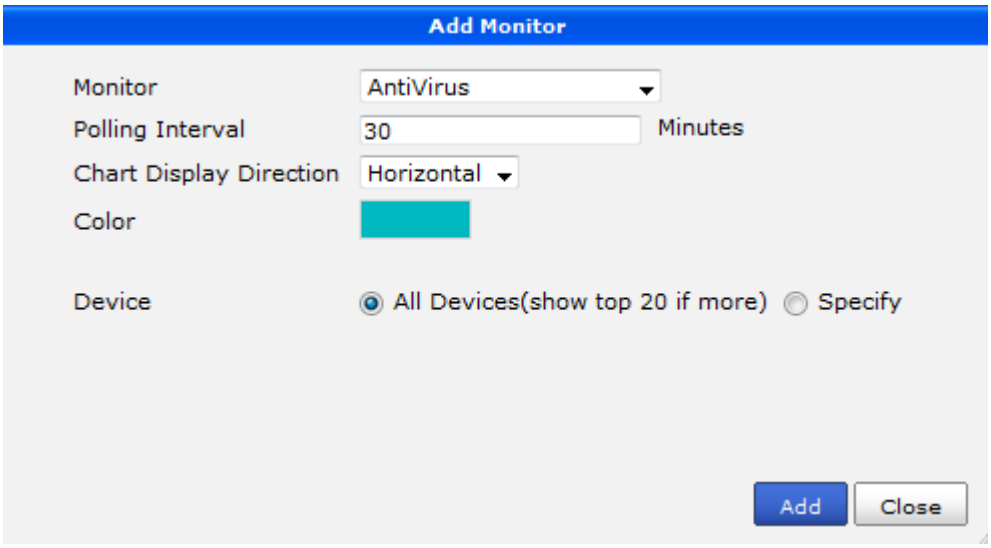


Resource, network, and threat monitors

A monitor allows you to watch the status of a variable associated with one or more monitored devices, such as CPU usage. You can set a high-water mark, or threshold, that will alert you when the device reaches a state that requires attention.

Go to *Real-time Monitor* > *Monitoring* > *Dashboard* and select *Add Monitor*.

Figure 169: Add Monitor window



The following information is displayed:

Monitor	Select the variable to monitor.
Polling Interval	Enter the frequency with which to request information from the monitored device. Polling more often generates more data but slows down the device a bit. The polling interval cannot be less than 5 minutes.
Chart Display Direction	Select *Horizontal* or *Vertical* from the drop-down list.
Color	Select the color for the chart.
Device	Select *All Devices*, or *Specify* to select individual devices.

FortiManager system alerts

Alerts provide a way to inform you of important issues that may arise on your devices and the FortiManager system itself based on the log messages that the FortiManager system collects. These alerts may be system failures or network attacks. By configuring alerts, you can easily and quickly react to such issues.

Alerts event

Alert events define log message types, severities and sources which trigger administrator notification.

You can choose to notify administrators by email, SNMP, or syslog.

To view configured alert events, go to *System Settings* > *Advanced* > *Alerts* > *Alerts Console*.

Figure 170: Viewing alert events

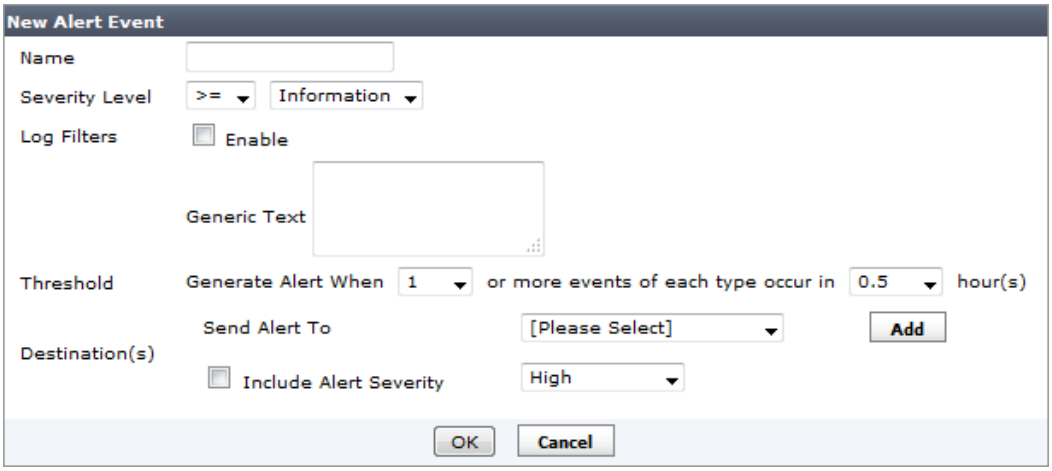
The following information and options are available:

Create New	Select to add a new alert event. For more information, see "To add an alert event:" on page 275.
#	The order the alert events were created.
Name	The name of the alert event.
Threshold	The number of events that must occur in the given interval before an alert is generated.
Destination	The location where the FortiManager system sends the alert message. This can be an email address, SNMP Trap or syslog server.
Delete icon	Select to remove an alert event.
Edit icon	Select to modify an alert event.

To add an alert event:

1. Go to *System Settings* > *Advanced* > *Alerts* > *Alerts Event,* and select *Create New*.

Figure 171: Adding alert events



2. Configure the following settings:

Name	Enter a unique name for the alert event.
Severity Level	Select the severity level to monitor for within the log messages, such as >=, and the severity of the log message to match, such as *Critical.* For example, selecting *Severity Level* >= *Warning*, the FortiManager system will send alerts when an event log message has a level of *Warning, Error, Critical, Alert* and *Emergency*. These options are used in conjunction with *Log Filters* to specify which log messages will trigger the FortiManager system to send an alert message.
Log Filters	Select *Enable* to activate log filters, and then enter log message filter text in the *Generic Text* field. This text is used in conjunction with *Severity Level* to specify which log messages will trigger the FortiManager system to send an alert message. Enter an entire word, which is delimited by spaces, as it appears in the log messages that you want to match. Inexact or incomplete words or phrases may not match. For example, entering log_i or log_it may not match; entering log_id=0100000075 will match all log messages containing that whole word. Do not use special characters, such as quotes (‘) or asterisks (*). If the log message that you want to match contains special characters, consider entering a substring of the log message that does not contain special characters. For example, instead of entering `User 'admin' deleted report 'Report_1'`, you might enter `admin`.
Threshold	Set the threshold or log message level frequency that the FortiManager system monitors before sending an alert message. For example, set the FortiManager system to send an alert only after it receives five emergency messages in an hour.
Destination	Select the location where the FortiManager system sends the alert message.

Send Alert To	Select an email address, SNMP trap or syslog server from the list. You must configure the email server and address, SNMP traps, or syslog server before you can select them from the list. For information on email server configuration, see For information on configuring SNMP traps, see For information on configuring syslog servers, see
Include Alert Severity	Select the alert severity value to include in the outgoing alert message information.
Add	Select to add the destination for the alert message. Add as many recipients as required.
Delete icon	Select to remove a destination.

3. Select *OK*.

Configuring alerts

When the FortiManager system receives a log message meeting the alert event conditions, it sends an alert message as an email, syslog message or SNMP trap, informing an administrator of the issue and where it is occurring.

You can configure the methods the FortiManager system uses to send alert messages. The FortiManager system can send an alert message to an email address via SMTP, a syslog server or as an SNMP trap.

Configuring alerts by mail server

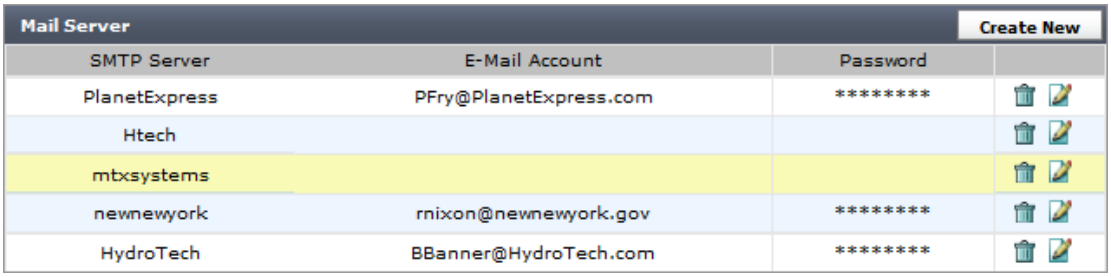
You must first configure an SMTP server to allow the FortiManager system to send mail alert messages.

If the mail server is defined by a domain name, the FortiManager system will query the DNS server to resolve the IP address of that domain name. In this case, you must also define a DNS server. See “Managing certificates” on page 74 to configure a DNS server.

If sending an email by SMTP fails, the FortiManager system will re-attempt to send the message every ten seconds, and never stop until it succeeds in sending the message, or the administrator reboots the FortiManager system.

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

Figure 172: Mail server list



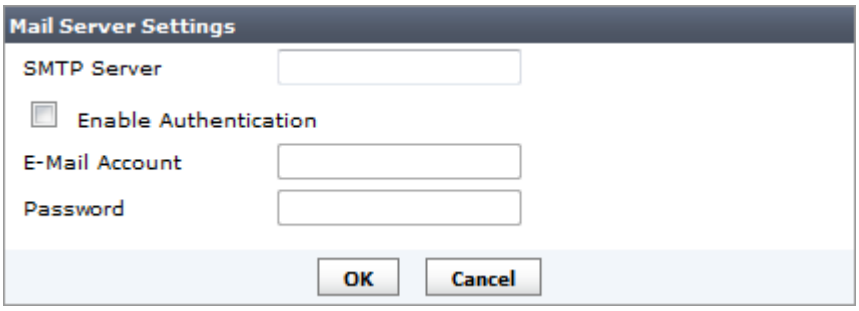
The following information and options are available:

Create New	Select to add a new mail server. For more information, see "To add a mail server:" on page 277.
SMTP Server	The SMTP server you have added.
E-Mail Account	The email address used for accessing the account on the SMTP server.
Password	The password used in authentication of that server. The password displays as ******.
Delete icon	Select to remove a mail server. This icon does not appear if the mail server is used by an alert event.
Edit icon	Select to modify a mail server.

To add a mail server:

1. Go to System Settings > Advanced > *Alerts* > *Mail Server* and select *Create New*.

Figure 173: Adding mail servers



2. Configure the following settings:

SMTP Server	Enter the name/address of the SMTP email server.
Enable Authentication	Select to enable SMTP authentication. When set, you must enter an email address and password for the FortiManager system to send an email with the account.

Email Account	Enter the user name for logging on to the SMTP server to send alert mails. You only need to do this if you have enabled the SMTPauthentication. The account name must be in the form of an email address, such as user@example.com.
Password	Enter the password for logging on to the SMTP server to send alert email. You only need to do this if you enabled SMTP authentication.

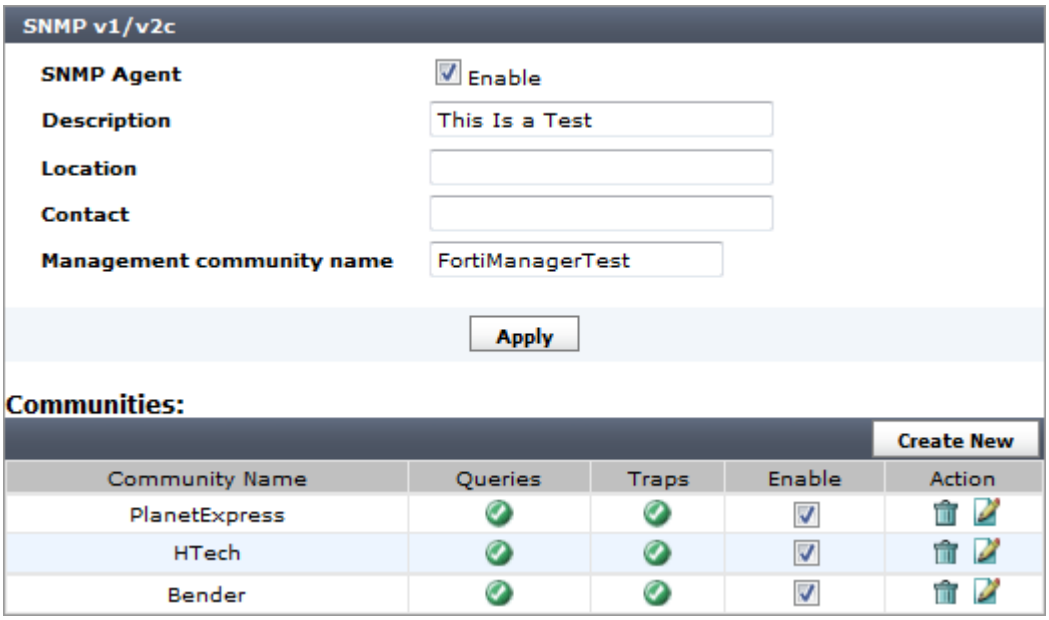
3. Select *OK*.

Configuring SNMP traps and alerts

You can configure the SNMP server where the FortiManager system sends SNMP traps when an alert event occurs, and which SNMP servers are permitted to access the FortiManager SNMP system traps. You must add at least one SNMP server before you can select it as an alert destination.

To view configured SNMP servers, go to *System Settings* > *Advanced* > *SNMP v1/v2.*

Figure 174:SNMP access list



The following information and options are available:

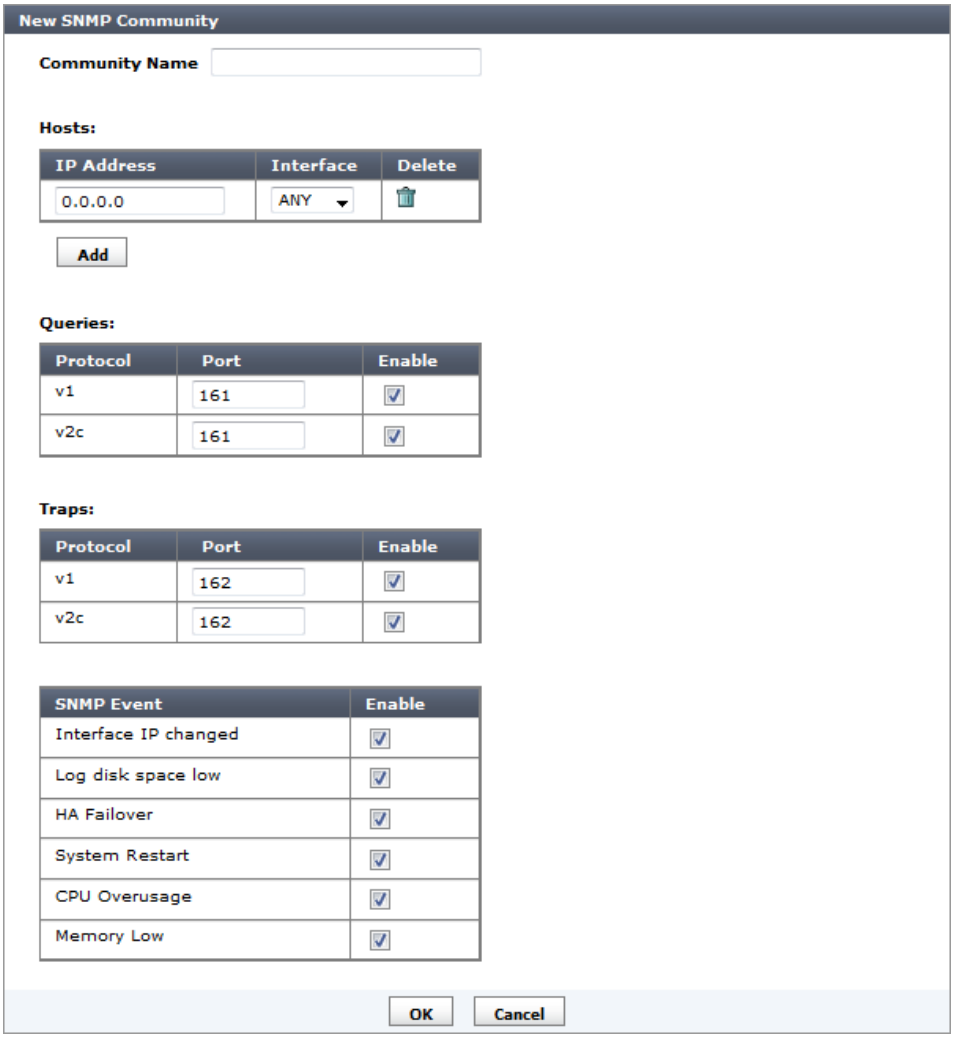
SNMP Agent	Select to enable the FortiManager SNMP agent. When this is enabled, it sends FortiManager SNMP traps.

	Description	Enter a description of this FortiManager system to help uniquely identify this unit.
	Location	Enter the location of this FortiManager system to help find it in the event it requires attention.
	Contact	Enter the contact information for the person in charge of this FortiManager system.
	Management Community Name	Enter the name to use for the community created by the FortiManager system during configuration of new FortiGate devices. The default value is FortiManager. This field can be a maximum of 127 characters long.
Communities		The list of SNMP communities added to the FortiManager configuration.
	Create New	Select to add a new SNMP community. If SNMP Agent is not selected, this control will not be visible. For more information, see "Configuring an SNMP community" on page 100.
	Community Name	The name of the SNMP community.
	Queries	The status of SNMP queries for each SNMP community.
	Traps	The status of SNMP traps for each SNMP community.
	Enable	Select to enable or unselect to disable the SNMP community.
	Delete icon	Select to remove an SNMP community.
	Edit icon	Select to edit an SNMP community.

To add a SNMP community:

1. Go to System Settings > Advanced > *SNMP v1/v2*.
2. Enable the SNMP Agent, select *Apply*. The option to *Create New* will appear under Communities. Select *Create New*.

Figure 175: Adding a SNMP community



3. Enter the *Community Name*.
4. Configure the *Hosts*, *Queries*, and *Traps* for the community.
5. Enable which SNMP events will generate alerts.

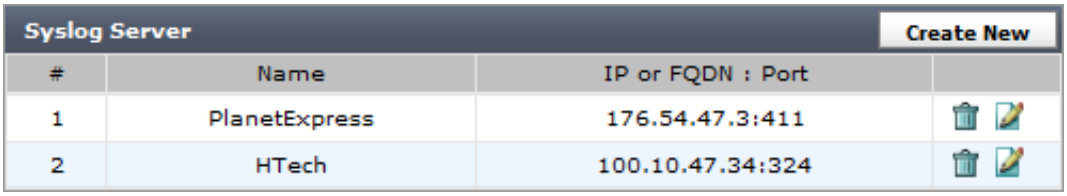
   Select from *Interface IP changed*, *Log disk space low*, *HA Failover*, *System Restart*, *CPU Overusage*, and *Memory Low*.
6. Select *OK*.

Configuring alerts by syslog server

You can configure syslog servers where the FortiManager system can send alerts. You must add the syslog server before you can select it as a way for the FortiManager system to communicate an alert.

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

Figure 176: Syslog server list



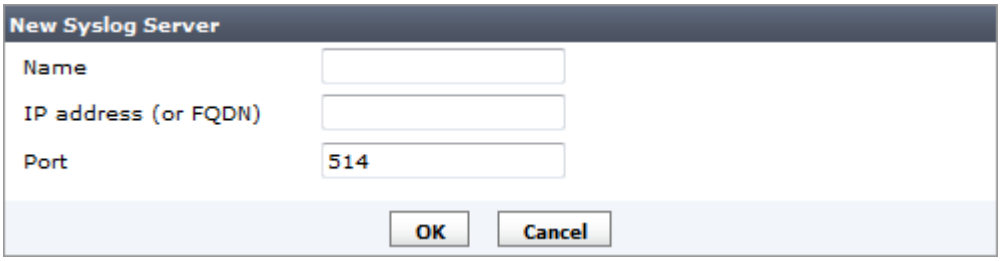
The following information and options are available:

Create New	Select to add a new syslog server. For more information, see "To add a mail server:" on page 277.
#	The order the syslog server was created.
Name	The IP address or fully qualified domain name for the syslog server, and port number.
Delete icon	Select to remove a syslog server. This icon does not appear if the syslog server is used by an alert event.
Edit icon	Select to modify a syslog server.

To add a syslog server:

1. Go to *System Settings* > *Advanced* > *Alerts* > *Syslog Server*.
2. Select *Create New*.
3. Enter the server name, IP address or FQDN, and port number.
4. Select *OK*.

Figure 177: Adding syslog Server

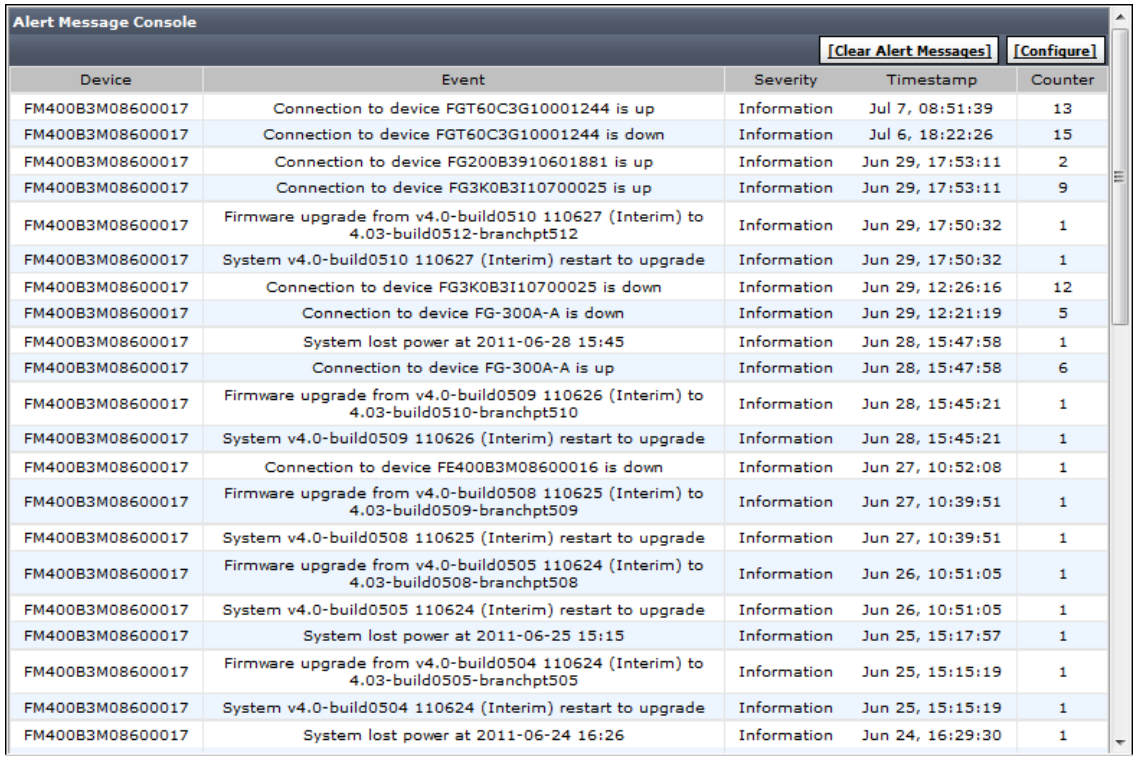


Alert console

The alert message console displays alert messages for the FortiManager system and connected devices, including hard disk failure messages, virus outbreak, or suspicious event warnings.

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

Figure 178: Alert message console



Device	Event	Severity	Timestamp	Counter
FM400B3M08600017	Connection to device FGT60C3G10001244 is up	Information	Jul 7, 08:51:39	13
FM400B3M08600017	Connection to device FGT60C3G10001244 is down	Information	Jul 6, 18:22:26	15
FM400B3M08600017	Connection to device FG200B3910601881 is up	Information	Jun 29, 17:53:11	2
FM400B3M08600017	Connection to device FG3K0B3I10700025 is up	Information	Jun 29, 17:53:11	9
FM400B3M08600017	Firmware upgrade from v4.0-build0510 110627 (Interim) to 4.03-build0512-branchpt512	Information	Jun 29, 17:50:32	1
FM400B3M08600017	System v4.0-build0510 110627 (Interim) restart to upgrade	Information	Jun 29, 17:50:32	1
FM400B3M08600017	Connection to device FG3K0B3I10700025 is down	Information	Jun 29, 12:26:16	12
FM400B3M08600017	Connection to device FG-300A-A is down	Information	Jun 29, 12:21:19	5
FM400B3M08600017	System lost power at 2011-06-28 15:45	Information	Jun 28, 15:47:58	1
FM400B3M08600017	Connection to device FG-300A-A is up	Information	Jun 28, 15:47:58	6
FM400B3M08600017	Firmware upgrade from v4.0-build0509 110626 (Interim) to 4.03-build0510-branchpt510	Information	Jun 28, 15:45:21	1
FM400B3M08600017	System v4.0-build0509 110626 (Interim) restart to upgrade	Information	Jun 28, 15:45:21	1
FM400B3M08600017	Connection to device FE400B3M08600016 is down	Information	Jun 27, 10:52:08	1
FM400B3M08600017	Firmware upgrade from v4.0-build0508 110625 (Interim) to 4.03-build0509-branchpt509	Information	Jun 27, 10:39:51	1
FM400B3M08600017	System v4.0-build0508 110625 (Interim) restart to upgrade	Information	Jun 27, 10:39:51	1
FM400B3M08600017	Firmware upgrade from v4.0-build0505 110624 (Interim) to 4.03-build0508-branchpt508	Information	Jun 26, 10:51:05	1
FM400B3M08600017	System v4.0-build0505 110624 (Interim) restart to upgrade	Information	Jun 26, 10:51:05	1
FM400B3M08600017	System lost power at 2011-06-25 15:15	Information	Jun 25, 15:17:57	1
FM400B3M08600017	Firmware upgrade from v4.0-build0504 110624 (Interim) to 4.03-build0505-branchpt505	Information	Jun 25, 15:15:19	1
FM400B3M08600017	System v4.0-build0504 110624 (Interim) restart to upgrade	Information	Jun 25, 15:15:19	1
FM400B3M08600017	System lost power at 2011-06-24 16:26	Information	Jun 24, 16:29:30	1

The following information and options are available:

Clear Alert Messages	Select to remove all alert messages.
Configure	Select to configure alert console settings including the period during which you want to display the messages and the severity level of the messages to be displayed. For example, selecting severity level *Warning* will display messages that have a level of *Warning, Notification,* and *Information*.
Device	The device where the alert message originates.
Event	The event causing the alert message.
Severity	The severity level of the alert message.
Timestamp	The date and time of the alert message.
Counter	

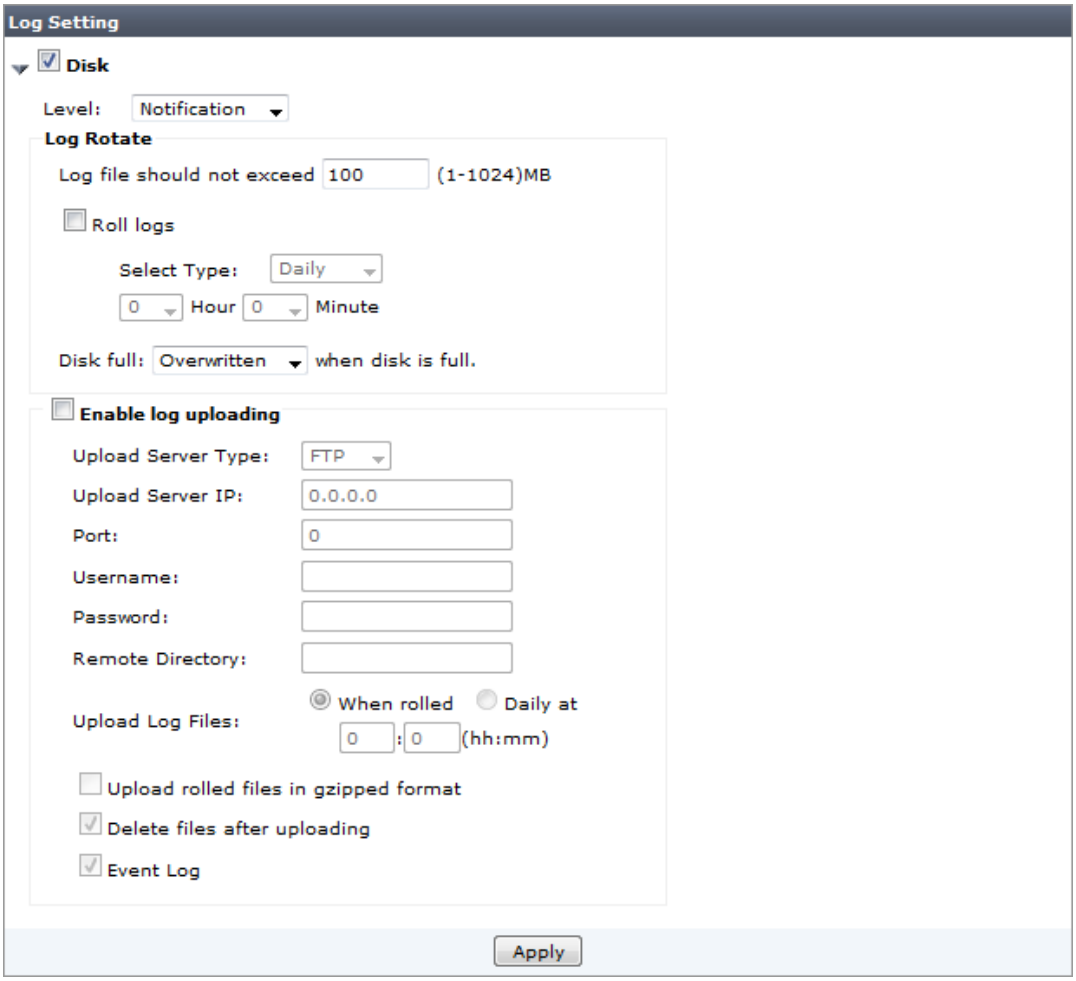
Device log

Information collected as part of Real-Time Monitor is saved to the Device Log. The Device Log is different from the FortiManager system logs.

Device log setting

To adjust device log settings, go to *System Settings* > *Advanced* > *Device Log* > *Log Setting*. When finished changing the settings, click *Apply*.

Figure 179: Device Log Setting



Configure the following settings:

Disk	Select to enable log setting configuration.
Level	Select the level of the notification from the drop-down list. Options include: *Emergency*, *Alert, Critical*, *Error, Warning*, *Notification*, *Information*, and *Debug*.
Log rotate	
Log file should not exceed	Enter the maximum log size in MegaBytes.
Roll Logs	Select to roll the logs. Rolling will occur either on a weekly or daily basis as selected.
Select Type	Select to roll the logs on a weekly or daily basis.
Select One Day	Select the day of the week to roll the logs. This option is enabled only when *Roll Logs* is selected and the *Type* is Weekly.
Hour, Minute	Select the Hour and Minute of the day to roll the logs. The hour is based on a 24 hour clock.

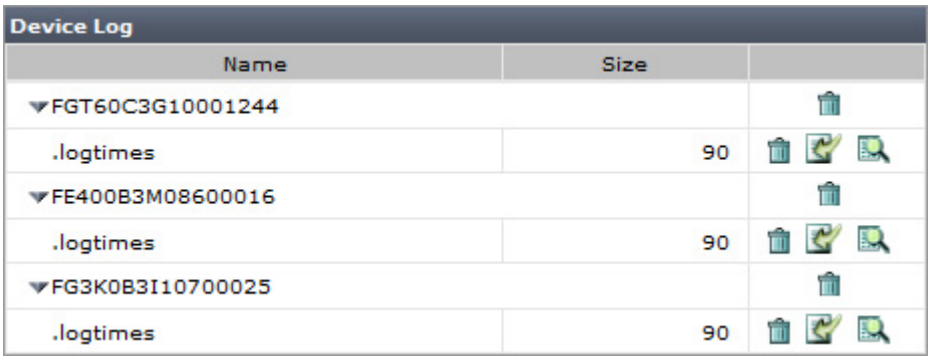
Disk Full	Select the action to take, *Overwritten* or *Do not log*, when the disk is full from the drop-down list.
Enable Log Uploading	Select to upload realtime device logs.
Upload Server Type	Select one of FTP, SFTP, SCP, or FAZ.
Upload Server IP	Enter the IP address of the upload server.
Port	Enter the port of the upload server.
Username	Select the username that will be used to connect to the upload server.
Password	Select the password that will be used to connect to the upload server.
Remote Directory	Select the remote directory on the upload server where the log will be uploaded.
Upload Log Files	
When Rolled	Select to upload log files when they are rolled according to settings selected under *Roll Logs*.
Daily at	Select the hour to upload the logs. The hour is based on a 24 hour clock.
Upload rolled files in gzipped format	Select to gzip the logs before uploading. This will result in smaller logs, and faster upload times.
Delete files after uploading	Select to remove device log files from the FortiManager system after they have been uploaded to the Upload Server.
Event Log	This option is not available.

Device log access

Go to *System Settings* > *Advanced* > *Device Log* > *Log Access*.

Accessing the device log follows the same method as accessing the FortiManager system logs.

Figure 180: Device Log Access



FortiClient Manager

Use the *FortiClient Manager* to centrally manage FortiClient endpoint security agents.

FortiManager v4.0 MR3 Patch Release 4 supports the following FortiClient versions:
FortiClient v4.0 and all Patch Releases
FortiClient v4.0 MR1 and all Patch Releases
FortiClient v4.0 MR2 and all Patch Releases

This section contains the following topics:

- FortiClient Manager maximum managed agents
- About FortiClient Manager clustering
- FortiClient Manager window
- Message center
- Working with clients (FortiClient agents)
- Working with FortiClient groups
- Managing client configurations and software
- Working with web filter profiles
- Configuring FortiClient manager system settings
- Configuring FortiClient manager clustering
- Configuring email alerts
- Configuring LDAP for web filtering
- Configuring FortiClient group-based administration
- Configuring enterprise license management
- Configuring FortiClient agent settings

FortiClient Manager maximum managed agents

The maximum number of FortiClient agents that *FortiClient Manager* can support depends on which FortiManager model you have.

Table 11: FortiClient Manager maximum managed FortiClient agents by model.

FortiManager model	Maximum number of managed FortiClient agents
FMG-100, FMG-100C	2500
FMG-400A, FMG-400B, FMG-400C	10000
FMG-1000C	25000
FMG-3000B	100000
FMG-3000C	120000
FMG-5001A	100000

The FortiManager system logs alerts when the number of managed FortiClient agents reaches 90 percent and 95 percent of the maximum. When the maximum is reached, the system raises an alert for every attempt to add another FortiClient agent. The FortiManager unit can continue to search for FortiClient agent, but it can add them only to the Temporary Clients list.

If the number of FortiClient agents that you want to support exceeds the capacity of your FortiManager unit, you can create a *FortiClient Manager* cluster of two or more FortiManager units. See "About FortiClient Manager clustering" on page 286.

About FortiClient Manager clustering

You can combine two or more FortiManager units into a *FortiClient Manager* cluster to manage a large number of FortiClient agents. One FortiManager unit is designated as the primary unit and all other units are secondary. The primary unit co-ordinates sharing of information amongst all units in the cluster. *FortiClient Manager* clustering uses TCP port 6028.

A managed FortiClient agent can log into any one of the units and receive its configuration information from that unit. Similarly, the administrator can log into any one of the units and modify the configuration of a FortiClient agent, even if that agent is connected to a different FortiManager unit.

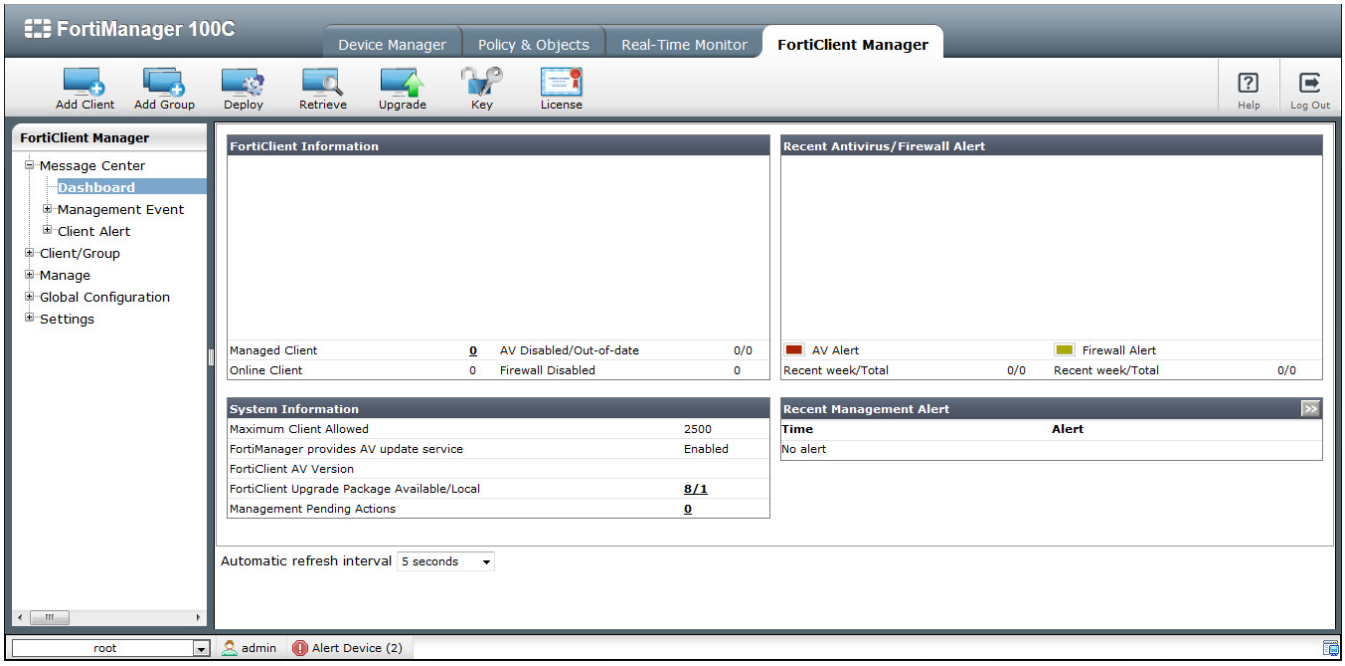
You must first select one FortiManager unit to act as the primary unit. After enabling clustering, register each secondary unit by entering its serial number and IP address. At each secondary unit, enable clustering and enter the IP address of the primary unit. For detailed information about configuring clustering, see "Configuring FortiClient manager clustering" on page 311.

FortiClient Manager window

The *FortiClient Manager* window is similar to other components of the FortiManager web-based user interface — a navigation pane is presented on the left side of the *FortiClient Manager* window, and when you select objects in the navigation pane, information and/or configuration options are displayed in the content pane of the *FortiClient Manager* window.

To view and configure FortiClient settings, select the *FortiClient Manager* tab in the menu bar.

Figure 181: FortiClient manager



Main menu bar

The main menu bar for *FortiClient Manager* is different from the default main menu bar. The buttons for *Device Manager* tasks are removed, and *FortiClient Manager* specific buttons are added.

Add Client	Select to add a FortiClient agent See “Searching for FortiClient agents” on page 297.
Add Group	Select to add a group of FortiClient agents. See “Adding a FortiClient agent group” on page 302.
Deploy	Select to install the configuration changes to the FortiClient groups and clients. See “Deploying FortiClient agent configurations” on page 306.
Retrieve	Select to retrieve configurations from FortiClient agents and save them in the FortiManager unit. See “Retrieving a FortiClient agent configuration” on page 306.
Upgrade	Select to Manage retrieval and deployment of FortiClient software upgrades. See “Working with FortiClient software upgrades” on page 307.
Key	Select to assign license keys to FortiClient groups. See “FortiClient license keys” on page 308.
License	Select to enable Enterprise licensing instead of standard fixed licensing. See “Configuring enterprise license management” on page 319.
Help **Log Out**	These buttons are the same as in the default Main Menu Bar. See “Using the main toolbar” on page 34.

Navigation pane

The *FortiClient Manager* portion of the navigation pane enables you to select and view the configuration options associated with FortiClient agents and groups.

Message Center	
Dashboard	View status information about *FortiClient Manager*. See "Dashboard" on page 290.
Management Event	Select the tabs to view information. *Management Event Summary* — View Management events, such as settings changes. See "Management event" on page 291. *Pending Action* — View pending actions for FortiClient agents. See "Viewing pending actions for FortiClient agents" on page 291. **Management Alert** — View a list of FortiClient computers that have licensing problems. See "Viewing management alerts for FortiClient agents" on page 292.
Client Alert	Select the tabs to view information. *Client Alert Summary* — View a brief listing of recent alerts and messages. **Firewall Alert** - View firewall alerts for FortiClient agents See "Viewing firewall alerts for FortiClient agents" on page 293. **Antivirus Alert** - View antivirus alerts for FortiClient agents. See "Viewing antivirus alerts for FortiClient agents" on page 294. **Upgrade Alert** - View information about failed FortiClient software upgrade attempts. See "Viewing upgrade alerts for FortiClient agents" on page 294.
Client/Group	Add FortiClient agents and organize them into client groups. See "Working with clients (FortiClient agents)" on page 295 and "Working with FortiClient groups" on page 301.
Client	Select this node to display all FortiClient agents managed by this FortiManager unit. This node is not visible to a FortiClient group administrator. There are four tabs: *Managed Client* - all managed clients. See "Viewing the clients lists" on page 295. *Ungrouped Client* - managed clients that do not belong to a client group. This node is not visible to a FortiClient group administrator that does not have access to ungrouped clients. *Temporary Client* - detected FortiClient agents that are not yet managed. This node is always empty if you selected the Client Discovery option Auto-populate managed clients list, which adds new clients to the Ungrouped Client node. This node is not visible to a FortiClient group administrator. *Unlicensed Client* - FortiClient agents with an expired or missing Enterprise license. **Free Edition Client**- FortiClient agents running the Free Edition Client.

Group	Select this node to display the FortiClient Group list. You can use the Client Group Tree to quickly navigate to the group or client that you want to configure.
Manage	
Deploy Configuration	Install the configuration changes to the FortiClient groups and clients. See “Deploying FortiClient agent configurations” on page 306.
Retrieve Configuration	Retrieve configurations from FortiClient agents and save them in the FortiManager unit. See “Retrieving a FortiClient agent configuration” on page 306.
FortiClient Upgrade	Manage retrieval and deployment of FortiClient software upgrades. See “Working with FortiClient software upgrades” on page 307.
FortiClient Key	Assign license keys to FortiClient groups. See “FortiClient license keys” on page 308.
Global Configuration	
Web Filter Profile	Create web filter profiles that you can apply to users and groups. See “Viewing and editing web filter profiles” on page 310.
Settings	
System	**System Setting:** Configure FortiClient discovery and lockdown settings. See “Configuring FortiClient manager system settings” on page 310. **Cluster Setting:** Configure settings to create a *FortiClient Manager* cluster. See “Configuring FortiClient manager clustering” on page 311. **Email Alert Setting:** Configure sending of email messages for management alerts and management events. See “Configuring email alerts” on page 312.
LDAP Integration	**LDAP Settings:** Configure settings to access LDAP servers. See “Configuring LDAP for web filtering” on page 313. **LDAP Group/User:** Assign web filter profiles to Windows AD users and groups. See “Working with Windows AD users and groups” on page 315.
Group Administration	Assign client groups to FortiClient group administrators. Available only to administrators with the Super_Admin profile. See “Configuring FortiClient group-based administration” on page 318.
Enterprise License	Enable Enterprise licensing instead of standard fixed licensing. “Configuring enterprise license management” on page 319.

Client group tree

When you go to *Client/Group* > *Group* in the *FortiClient Manager*, you see the Client Group Tree immediately to the right of the navigation pane. Client groups and their subgroups are clearly displayed. You can select a client group to configure. To provide more space in the content pane, you can collapse the Client Group Tree panel.

At the top of the client group tree is a toolbar that controls the appearance of the tree view.

Expand All	Expand all nodes in the tree
Collapse All	Collapse All nodes in the tree
Refresh Tree	Update the tree from the *FortiClient Manager* database

FortiClient menu

When you select a client group or a FortiClient agent to configure, the FortiClient menu is visible at the left side of the content pane. You use the FortiClient menu to select different parts of the FortiClient configuration for editing.

The FortiClient menu and configuration pages differ from the FortiClient application. See "Configuring FortiClient agent settings" on page 321 for detailed information about configuring these settings.

Message center

The Message Center provides status information about the FortiClient agents in your network.

- Dashboard — statistical information and recent activity
- Management event — management events and alerts, pending actions
- Client alert — client firewall, antivirus and update alerts

Dashboard

The *FortiClient Manager* dashboard provides the following information:

FortiClient Information	Provides counts of • managed clients (select count to see Managed Clients list) • managed clients currently online (number and percentage) • clients at risk due to disabled or outdated antivirus protection (number and percentage) • clients with firewall disabled
System Information	
Maximum Client Allowed	The maximum number of managed FortiClient agents. This depends on the FortiManager model. See "FortiClient Manager maximum managed agents" on page 285.
FortiManager provides AV update service	The status (enabled or disabled) of *FortiClient Service* in *FortiGuard AV & IPS Settings*. For more information, see "FortiGuard Services" on page 242.

FortiClient AV Version	The current antivirus engine and signatures versions provided by FortiGuard Center.
FortiClient Upgrade Package Available/Local	The number of FortiClient software upgrade packages available from FortiGuard and on this FortiManager unit. Select the count to view the FortiClient Upgrade page. See "Working with FortiClient software upgrades" on page 307.
Management Pending Actions	The number of pending actions on all managed FortiClient agents. Select the count to view the *All Pending Actions* list. For more information, see "Viewing pending actions for FortiClient agents" on page 291.
Recent Management Alert	The most recent management alerts. Click the >> button to view the *All Management Alert* list. For more information, see "Viewing management alerts for FortiClient agents" on page 292.
Recent Antivirus/Firewall Alert	A graph showing the number of antivirus and firewall alerts over the past week.
Recent Event Message	Recent event messages. Click the >> button to view the *All Event Logging* list. For more information, see "Management event" on page 291.
Automatic refresh interval	Sets how often *FortiClient Manager* updates dashboard information.

Management event

In *FortiClient Manager*, go to *Message Center* > *Management Event* to view:

- Management Event Summary
- Pending Action
- Management Alert

The Management Event Summary page shows lists of the most recent alerts and events. You can also view a count of the total pending actions. For more detailed information, click the >> button in the list title bar. You can also select the Pending Action, Management Alert and Management Event tabs at the top of the content pane.

Viewing pending actions for FortiClient agents

Go to *Message Center* > *Management Event* > *Pending Action* to view the All Pending Actions page. This page displays actions that cannot be executed instantly because the FortiClient agent is offline or otherwise unreachable. Actions are removed from the list as they are successfully completed.

View per Page	Select the number of clients to display per page.
Line	Enter the line of the list that you want to view and select Go.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.

Last page icon	Go to last page.
Find Hostname	Enter the hostname and select *Go* to move to the first entry for the host.
#	Line numbers
FortiClient	The name of the FortiClient agent with pending action.
Action	The action items to be executed.
Information	The most up-to-date AV Signature/AV engine version numbers on the FortiManager unit. This information only applies to the Notify AV engine/database upgrading action.
Time	Date and time when the pending action item was created.
Delete	Delete the selected pending action manually.
Delete All	Delete all pending actions.

Viewing management alerts for FortiClient agents

In the *FortiClient Manager*, go to *Message Center* > *Management Event* > *Management Alert* to view a list of FortiClient agents that have licensing problems.

View per page	Select the number of lines to display per page: 25, 50, 100, or 1000
Line	Optionally, enter a line number and select Go to start the page with that line.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.
Find Alert	Optionally, enter search text and select Go.
#	Alerts are numbered in the order they occur.
Time	The time of the alert.
Alert	Description of the alert.
Action	Delete icon - Delete this alert.
Delete	Delete the selected alerts.
Delete All	Delete all the listed alerts.

Client alert

Go to *Message Center* > *Client Alert* in *FortiClient Manager* to view the following messages from FortiClient agents:

- firewall alerts
- Antivirus alerts
- upgrade alerts

Client alert summary

The Client Alert Summary page shows lists of recent firewall and antivirus alerts. For more detailed information, select the >> button in the list title bar. You can also select the *Firewall Alert*, *AntiVirus Alert* and *Upgrade Alert* tabs at the top of the content pane.

The Client Alert Summary page also shows statistical information about the number of alerts received from FortiClient agents. For more detailed information, select the count. For example, if you select the count for AV Alert Total, you view the All Antivirus Alerts page.

Viewing firewall alerts for FortiClient agents

In the *FortiClient Manager*, go to *Message Center* > *Client Alert* > *Firewall Alert* to view violations of firewall policies on your FortiClient agents.

View per Page	Select the number of clients to display per page.
Line	Enter the line of the list that you want to view and select Go.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.
Find Address/Service	To find a particular IP address or firewall service in the list, enter it in this field and select Go.
#	Line numbers
Host Name	Host name of FortiClient agent.
Client IP	IP address of FortiClient agent.
Direction	Inbound or Outbound direction of violation traffic.
Source/Destination	Source (inbound) or destination (outbound) of violating traffic.
Service/Port	Firewall service in which violation occurred and the TCP or UDP port number are listed.
# Violation	The number of times this violation has occurred.
Last Violation	The time of the latest violation of this type.
Delete icon	Select to delete violation record.
Delete All	Delete all violation records.

Viewing antivirus alerts for FortiClient agents

In the *FortiClient Manager*, go to *Message Center* > *Client Alert* > *AntiVirus Alert* to view a list of the viruses detected on FortiClient agents.

View per Page	Select the number of lines to display per page.
Line	Enter the line of the list that you want to view and select Go.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.
Find Virus/Filename	Enter the name of a virus or a file and select Go to search for it.
#	Viruses are numbered in the order they are found.
Host Name	The host where the virus was found.
Time	The time when the virus was found.
Virus	The name of the virus.
Filename	The name of the virus-infected file.
Delete	Delete the selected virus alerts.
Delete All	Delete all the virus alerts.

Viewing upgrade alerts for FortiClient agents

In the *FortiClient Manager*, go to *Message Center* > *Client Alert* > *Upgrade Alert* to view a list of FortiClient agents that have software upgrade problems.

View per page	Select the number of lines to display per page: 25, 50, 100, or 1000
Line	Optionally, enter a line number and select Go to start the page with that line.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.
Find Hostname	Optionally, enter the host name and select Go to display only the alerts for that FortiClient agent.
#	Upgrade alerts are numbered in the order they occur.
Host Name	The host name of the affected FortiClient agent.
Client IP	The IP address of the FortiClient agent.

Time	The time of the alert.
Expected Version ID	The expected current software version on the FortiClient agent.
Error Description	Information about the upgrade alert.
Delete	Delete the selected upgrade alerts.
Delete All	Delete all the listed upgrade alerts.

Working with clients (FortiClient agents)

This section describes how to search, add and delete FortiClient agents. For information about configuring FortiClient agents individually or in groups, see "Configuring FortiClient agent settings" on page 321. This section includes the following topics:

- Searching for FortiClient agents
- Adding or removing temporary clients
- Removing or relicensing unlicensed clients
- Deleting FortiClient agents
- Viewing the clients lists
- Filtering the clients list

Viewing the clients lists

Go to *Client/Group* > *Client* > *Managed Client* in the *FortiClient Manager* navigation pane to view the list of all managed FortiClient agents. For each agent, you can edit the description and modify the full configuration. The columns displayed depend on the Columns Display setting.

You can also set the *Display* to *Ungrouped Client* to view only the FortiClient agents that are not members of a client group.

Display	Select the group of FortiClient agents to list. By default, all FortiClient agents are listed.
Search/Add New	Find FortiClient agents on the network. This is only available when viewing the All FortiClient list. See "Searching for FortiClient agents" on page 297.
View per Page	Select the number of clients to display per page.
Line	Enter the line of the list that you want to view and press Enter.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.
Find Hostname/IP	To find a particular FortiClient computer in the list, enter the host name or IP address and select Go.

Columns Display	Select the which columns to display in this list. You can also restore the default set of columns.
Columns Filter	Apply filters to display a subset of managed clients. See “Filtering the clients list” on page 297.
#	Line number. The number is black if the FortiClient agent has a Standard Fixed license, blue if it has an Enterprise license.
The *Columns Display* setting determines which of the following columns are displayed.	
Host Name	FortiClient agent host name. You can select the host name to access configuration settings for the FortiClient agent.
IP Address	IP address of FortiClient agent.
OS	Operating system of FortiClient agent.
DNS Domain	DNS domain name of FortiClient agent.
Windows Workgroup	Windows domain or workgroup of FortiClient agent.
Serial No	Serial number of FortiClient agent.
Version	FortiClient software version of FortiClient agent.
Expiry Date	License expiry date of FortiClient agent.
Last AV Update Check	Time of last check for updated AV signatures.
Status	Status indicators for Online, antivirus, Firewall, VPN. Green up arrow indicates up/operational. Red down arrow indicates not operational.
AV Update Status	Status indicators for antivirus engine and database.
Roaming	A checkmark indicates that Roaming is enabled for this client.
Membership	The client group to which the FortiClient agent belongs.
Action	
Delete icon	Delete the FortiClient agent from the database.
Edit icon	Edit the description for FortiClient agent.
Revoke icon	Revoke the enterprise client license of this FortiClient agent and move the FortiClient agent to the Unlicensed Clients list. See “Removing or relicensing unlicensed clients” on page 299.

Group To	Change the group to which the selected agents belong. Select the agents, select the group, and then select *Group To*.
Allow Roaming	Change the roaming status of the selected FortiClient agents. Roaming agents are dynamically grouped when they change IP address. *FortiClient Manager* sends the new group configuration to the FortiClient agent. Select agents, select *Enable* or *Disable*, and then select *Allow Roaming*.

Filtering the clients list

When viewing the *All Managed Clients* or *Ungrouped Clients* list, you can define filters to reduce the list by including or excluding agents based on column values. For example, you could display only the FortiClient agents on a particular subnet.

To filter the client list:

1. In the *FortiClient Manager*, in the *Managed Client* list or the *Ungrouped Client* list, select the *Columns Filter* icon.

   The *Columns Filter* dialog opens.
2. Select the column(s) that you want to filter and enter the criteria for inclusion in the list.
3. Select *OK*.

To turn off column filtering:

1. In the *FortiClient Manager*, in the *Managed Client* list or the *Ungrouped Client* list, select the *Columns Filter* button.

   The *Columns Filter* dialog opens.
2. Clear the check box of each column you no longer want to filter, or select *Clear* to end all column filtering.
3. Select *OK*.

Searching for FortiClient agents

To add FortiClient computers to the FortiManager unit database, you must search the network for computers running FortiClient software. You can search for a single computer or multiple agents in the network.

If in *FortiClient Manager Settings* > *System* > *System Setting* you selected *Auto-populate managed client list*, the discovered FortiClient agents are added to the FortiManager unit as managed clients. Otherwise, the discovered clients appear in the Temporary Clients list. See “Client Discovery” in “Configuring FortiClient manager system settings” on page 310. You can view the temporary clients and add them to the FortiManager unit at any time.

By default, *FortiClient Manager* adds discovered FortiClient agents to the *Ungrouped Client* list. If you selected the *Add to temporary clients list* option in the *Client*

Discovery settings, *FortiClient Manager* adds discovered FortiClient agents to the Temporary Clients list. You cannot configure temporary clients until you add them to the list of managed clients. See “Adding or removing temporary clients” on page 298.

To search and add FortiClient agents:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client*.
2. In the All Managed Clients list, select *Search/Add New*.
3. To search a single agent, select *Lookup single client (IP/FQDN)* and enter the agent's IP address or FQDN.
4. To search multiple agents, select *Scan attached networks*.
   - Select the *Interface* through which the FortiManager unit is connected to the network(s).
   - Select the *Network (IP/Mask)* from which you want to search for FortiClient agents.
5. Select *Search*.

   The discovered agents are listed with hostnames and IP addresses.
6. To add the discovered agents to the FortiManager unit, do one of the following and select *Add to Managed*:
   - To add all discovered agents, select the check box at the top.
   - To add a single discovered agent, select the check box before the agent in the list.

   If *Auto-populate managed client list* is enabled in FortiClient global settings, the discovered agents are automatically added to the database and the *Add to Managed* button is not available.

To view and add temporary FortiClient agents:

1. In the *FortiClient Manager*, select *Client Group* > *Client* > *Temporary Client*.
2. To add listed agents to the FortiManager unit, do one of the following and select *Add to Managed*:
   - To add all discovered agents, select the check box at the top.
   - To add a single discovered agent, select the check box before the agent in the list.
3. To remove agents from the temporary FortiClient agent list, do one of the following and select *Delete*:
   - To delete all agents, select the check box at the top.
   - To delete a single agent, select the check box before the agent in the list.

Adding or removing temporary clients

Newly-discovered FortiClient agents are listed in the Temporary Clients list if you selected the Add to the temporary clients list option in *FortiClient Manager* system settings. (See "Client Discovery" in "Configuring FortiClient manager system settings" on page 310.)

You can add temporary clients to the managed clients list or delete them.

View per page	Select the number of lines to display per page: 25, 50, 100, or 1000
Line	Optionally, enter a line number and select Go to start the page with that line.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.

Find Hostname/IP	Optionally, enter the host name and select Go to display only that client.
#	Temporary clients are numbered.
FortiClient	Host name of the FortiClient agent.
IP Address	IP address of the FortiClient agent.
OS	Operating system of the FortiClient agent.
DNS Domain	DNS/domain name of the FortiClient agent.
Discovery Method	The method used to discover the FortiClient agent. One of: *FortiClient Register* — FortiClient agent registered directly *FortiManager Scan Search* — FortiManager searched the network *FortiClient Query* — FortiClient agent sent discovery query on network *FortiManager Lookup Client* — FortiManager searched the network with a single client IP address
Add to Managed	Move the selected FortiClient agent to the Ungrouped Clients list.
Delete	Remove the selected FortiClient agent from the Temporary Clients list.
Delete All	Remove all FortiClient agents from the Temporary Clients list.

To add temporary FortiClient agents:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Temporary Client*.
2. Select the agents you want to add.
3. Select *Add to Managed*.

   The FortiClient agents are added to the *All Managed Clients* and *Ungrouped Clients* lists.

To delete temporary FortiClient agents:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Temporary Client*.
2. Select the agents you want to remove
3. Select *Delete*.

Removing or relicensing unlicensed clients

If you are using Enterprise redistributable licensing and you revoked a client's license, that client is listed in the Unlicensed Client list. Go to *Client/Group* > *Client* > *Unlicensed Client* to view the list of unlicensed clients.

View per page	Select the number of lines to display per page: 25, 50, 100, or 1000
Line	Optionally, enter a line number and select Go to start the page with that line.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.

Last page icon	Go to last page.
Find Hostname/IP	Optionally, enter the host name and select Go to display client.
#	Temporary clients are numbered.
FortiClient	Host name of the FortiClient agent.
IP Address	IP address of the FortiClient agent.
OS	Operating system of the FortiClient agent.
DNS Domain	DNS/domain name of the FortiClient agent.
Discovery Method	The method used to discover the FortiClient agent. One of: *FortiClient Register* — FortiClient agent registered directly *FortiManager Scan Search* — FortiManager searched the network *FortiClient Query* — FortiClient agent sent discovery query on network *FortiManager Lookup Client* — FortiManager searched the network with a single client IP address
Grant	Re-grant the FortiClient agents client license.
Delete	Remove the selected FortiClient agent from the Unlicensed Clients list.
Delete All	Remove all FortiClient agents from the Unlicensed Clients list.

Deploying licenses to standard edition clients

You can view the agents running the Standard (Free) edition of FortiClient on the Free License Clients tab. The Free edition of FortiClient are those agents running FortiClient but do not have licenses. You can deploy licenses so they will be upgraded to the Premium edition. With the Premium edition, all features are “unlocked’ and the clients can be managed via FortiManager.

To deploy licenses to free edition clients:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Free Edition Client.*
2. Select the client you want to deploy a license.
3. Enter the license number and click *Deploy License*.

Deleting FortiClient agents

You can delete FortiClient agent records from the FortiManager unit. If the agent belongs to a client group, it will be removed from the group.

To delete agents:

1. In the *FortiClient Manager*, from the Main Menu Bar, select *Client/Group* > *Client* > *Managed Client*.
2. Select FortiClient agents from the list.
3. Select *Delete*.

Working with FortiClient groups

You may want to divide the managed FortiClient agents into groups in order to:

- Configure group-shared settings and then install the configurations on the agents all at once.
- Group FortiClient agents according to IP address, Windows Workgroup, DNS domain or operating system.
- Manage a large number of agents more efficiently.

Each FortiClient agent can be added to only one group.

Overview of client groups

FortiClient Manager supports both statically and dynamically populated groups. Groups can be nested to help you organize your FortiClient agents for convenient management. A FortiClient agent can belong to only one group.

Static client group

A static group has a fixed membership that you define by selecting group members manually. When a FortiClient agent belongs to a static group, it cannot become a member of a dynamic group even if it matches the criteria.

Dynamic client group

A dynamic group has members who match one of the following criteria:

- the computer's IP address, IP address range or subnet
- the computer's DNS domain
- the operating system of the computer
- the Windows Workgroup to which the computer belongs
- the FortiClient agent's Enterprise Client License

The *FortiClient Manager* compares agents to the criteria of each dynamic group starting at the top of the list of groups. The agent is assigned to the first group that it matches. This dynamic grouping process runs when

- you add a new FortiClient agent to the managed list
- you edit or add a new dynamic group
- you select *Refresh* while editing a FortiClient group

Dynamic grouping applies to

- ungrouped agents
- agents that are members of dynamic groups
- agents that have roaming enabled

Nested groups

You can create groups of groups. To assign a group as a member of another group, you select that group as the parent group. For example, to make Group B a member of Group A, when you configure Group B you select Group A as the parent group.

Dynamic groups can be members of static groups and vice versa. Nesting is limited to eight levels in depth.

Viewing FortiClient groups

Select *Client/Group* > *Group* in the *FortiClient Manager* navigation pane to view the FortiClient Group list.

Add	Create a new FortiClient group. See "Adding a FortiClient agent group" on page 302.
Refresh Dynamic Grouping	Recreate dynamic groups based on their criteria.
Name	FortiClient group name. Select to edit FortiClient settings for the group.
Member	The number of members in the group. This does not include members of nested groups.
Description	Optional description of the group.
Type	Static or Dynamic. For more information, see "Overview of client groups" on page 301.
Action	
Delete icon	Delete this group.
Edit icon	Edit the group membership and settings. For information about fields, see "Adding a FortiClient agent group" on page 302.

Adding a FortiClient agent group

In the *FortiClient Manager*, to add a client group, select *Client/Group* > *Group* in the navigation pane and then select *Add* in the content pane. Enter the required information and select *OK*.

Group Name	Enter a unique *Group Name*. The name cannot be the same as the name of another agent or agent group.
Description	Enter a *Description* for the agent group. You can use the description to provide more information about the FortiClient agent group. For example, you could include its location or any other useful information.

Redirect FortiManager IP	This field is available only if clustering is enabled. In a *FortiClient Manager* cluster, this is the address of the *FortiClient Manager* where FortiClient agents in this group should log on. FortiClient agents can log on to the primary server in the cluster but are redirected to this specified secondary server. A value of 0.0.0.0 disables redirection.
FortiManager Serial Number	Enter the serial number of the FortiManager unit. This is necessary only if the FortiClient agent or the FortiManager unit is behind a NAT device. If a FortiManager cluster manages the group, enter the serial numbers of both units separated by a comma.
Parent Group	To create a nested group, select the group to which this group belongs.
Group Order	Select an existing group from the list and choose whether the new group appears before or after that group in the navigation pane.
Group Type	Select *Static Group* to manually group agents using the Group Members list. Select *Dynamic Group* to group agents based on the *Policy*.
Policy	For a dynamic group, select the criteria for membership in this client group. One of:
DNS domain	Type the DNS domain name or select it from the *Select* list.
Operating System	Type the operating system name or select it from the *Select* list.
Windows Workgroup	Type the Windows Workgroup name or select it from the *Select* list.
IP Range/Subnet	Enter an IP address, an IP address range such as 192.168.1.2-192.168.1.5, or a subnet address such as 192.168.1.0/24. You can specify multiple address criteria if you enter them as separate lines.
Enterprise Client License	Type the Enterprise Client License key.

You add clients to the group by using the *Group To* button in the All Managed Clients list. See "Viewing the clients lists" on page 295.

Deleting a FortiClient agent group

You can delete a single group, multiple groups, or all the groups at once. This does not delete the member devices.

To delete agent groups:

1. In the *FortiClient Manager*, select *Client/Group* > *Group*.
2. Select the group or groups you want to delete, then select *Delete*.
3. If you want to delete all the groups, select *Delete All*.

Editing a FortiClient agent group

You can modify group description, adjust group order, and change group type.

To edit a client group:

1. In the *FortiClient Manager*, from the navigation pane, select *Client/Group* > *Group*.
2. Select the client group that you want to modify.
3. Select *Edit*.
4. Make the changes and select *OK*.

Viewing group summaries

In the navigation pane, go to *FortiClient Manager* > *Client/Group* > *Group*. In the FortiClient menu, go to *System* > *Status* to view the high level information for the group.

Edit	Edit client group configuration.
Apply to all members	Apply group settings to all members, eliminating overrides.
Group Name	The name of the FortiClient agent group.
Description	Descriptive notes about the FortiClient agent group.
Group Type	The type of FortiClient agent group: Static Group - manually selected members Dynamic Group - membership based on IP address, domain, Windows Workgroup or operating system
Redirect FortiManager IP	If clustering is enabled, this is the address of the secondary *FortiClient Manager* to which FortiClient agents are redirected. A value of 0.0.0.0 means that clustering or redirection is disabled. “About FortiClient Manager clustering” on page 286.
Redirect FortiManager SN	This is the serial number of the secondary *FortiClient Manager* to which FortiClient agents are redirected. See Redirect FortiManager IP, above.
Group Members	Member FortiClient agents in this group, including their hostnames and IP addresses.
Apply	Select to save the FortiClient agent group.

Configuring settings for client groups

You can select a FortiClient agent group and configure the settings shared by all the agents in this group, including trusted FortiManager units, firewall, VPN, antivirus, web filter, and logs.

The configuration steps are identical to configuring a single managed FortiClient agent, except that group settings apply to all members in the group and that, in most cases, there is no override function in group configurations. See “Configuring FortiClient agent settings” on page 321.

The override server configuration under web filter is the only override function associated with group settings. Once you select the override options and complete the configuration, the FortiClient agents will get the Web Filtering and email filtering settings from the FortiManager unit instead of from the FortiGuard server through the Internet. See "Configuring web filter options on a FortiClient agent" on page 351.

After completing a configuration for a group or a member FortiClient agent configuration, you can copy the group configuration to other groups or the member FortiClient agent configuration to the group to which it belongs.

The group and member configurations that can be copied include:

- System > Trusted FMGs
- Firewall > Policies/Addresses/Service/Schedules
- VPN
- Anti Virus > Scheduled Scans

You can override specific group settings in a group member's configuration. In the group configuration you can reapply the group settings to all members.

To copy a group configuration to other groups:

1. In the *FortiClient Manager*, go to *Client/Group* > *Group* and select a FortiClient group in the *Client/Group Tree*.
2. From the FortiClient menu, select the configuration that you want to copy, for example Firewall > IP Address.
3. From the *Action* column, select the *Copy to other group(s)* icon.
4. Select the target group(s) to which you want to copy a group configuration.
5. Select one of the options for *When same name configuration exists in export-to group(s): Overwrite* or *Keep unchanged*.
6. Select *OK*.

To reapply group settings to all members:

1. In the *FortiClient Manager*, go to *Client/Group* > *Group* and select a FortiClient group in the Client/Group Tree.
2. From the FortiClient menu, select the configuration that you want to apply to all of the group members, for example Firewall > IP Address.
3. Do one of the following:
   - From the *Action* column, select the setting's *Apply to member(s)* icon.
   - To apply all settings on the configuration page to all group members, select *Apply to All Members* at the top of the page.
4. Select *OK* to confirm copying the configuration.

To export a member configuration to its parent group:

1. In the *FortiClient Manager*, go to *Client/Group* > *Group* and select a FortiClient group in the Client/Group Tree.
2. In the *Group Members* list, select a member.
3. From the FortiClient menu, select the configuration that you want to copy to the group, for example Firewall > IP Address.
4. Select *Override*.
5. Select the *Copy to group* icon for the configuration that you want to export.

Managing client configurations and software

Using *FortiClient Manager*, you can

- deploy configurations to FortiClient agents
- retrieve configurations from newly-added FortiClient agents
- make software upgrades available to FortiClient agents
- manage the licensing of FortiClient software

Deploying FortiClient agent configurations

After you make configuration changes, you can deploy the changes to the FortiClient agents. Before you deploy them, all the changes are stored in the FortiManager database.

Deployment may fail if you make configuration changes on the computer at the same time. For details, see "Retrieving a FortiClient agent configuration" on page 306.

To deploy configuration changes to client groups:

1. In the *FortiClient Manager*, select *Manage* > *Deploy Configuration* in the Main Menu Bar.
2. Select one of these options:

   Deploy all configuration changes — Deploy changes to all affected FortiClient agents.

   Deploy configuration changes for FortiClient agents in selected groups — FortiClient agents in child groups of the selected group are not affected.

   Deploy configuration changes for FortiClient agents in selected groups and child groups — Changes are also deployed to FortiClient agents in child groups of the selected group.
3. Unless you selected *Deploy all configuration changes*, select the groups to which you want to deploy the changes.
4. Select *Deploy*.

To deploy configuration changes to individual FortiClient agents:

1. In the *FortiClient Manager*, select *Manage* > *Deploy Configuration* in the Main Menu Bar.
2. Select the *Deploy Configuration to Client* tab.
3. Select the FortiClient agents to which you want to deploy the updated configuration.

   If you select the check box in the table heading, all FortiClient agents are selected.
4. Select *Deploy*.

Retrieving a FortiClient agent configuration

After you add a FortiClient agent to the FortiManager system, you can resynchronize with the agent by retrieving the FortiClient configuration from the agent and saving it to the FortiManager database.

After resynchronization, if you make any FortiClient configuration changes on the agent rather than through the FortiManager System, the configuration on the agent and the configuration saved in the FortiManager database will be out of sync. In this case, you can resynchronize the agent again.

The installation of configuration changes to a agent may fail if you make configuration changes on the agent at the same time.

To resynchronize an agent:

1. In the *FortiClient Manager*, select *Manage* > *Retrieve Configuration* in the Main Menu Bar.
2. Select the agents that you want to resynchronize, then select *Retrieve*.

   The resynchronization process may take a few minutes, depending on network speed.

Working with FortiClient software upgrades

The FortiManager unit can update FortiClient application installations with software updates retrieved from the FortiGuard service. In the *FortiClient Manager*, go to *Manage* > *FortiClient Upgrade* to view the available upgrade packages.

Delete All	Delete all of the listed upgrade packages.
Refresh	Update the list.
Import	Manually import a software package. This is used to add customized FortiClient installation packages to the *Imported Package* list. For more information, see "Importing a software upgrade package" on page 307.
Version	The major version and build number. For example, 4.2.5.0286 is version 4.0, major release 2, patch release 5, build 0286.
Platform	One of: WIN 32 ENT: Windows 32-bit Enterprise edition WIN 64 ENT: Windows 64-bit Enterprise edition
Date	The date and time when the software upgrade was released.
Status	For official released packages only. One of: Ready: the software upgrade is ready to download from FDS. Accept: download requested Processing: *FortiClient Manager* is downloading the software upgrade Downloaded: imported software upgrade is ready to deploy Failed: download of software upgrade failed
Description	A description of the package.
Action	Download: download the software upgrade Deploy: deploy software upgrade to clients Delete: delete the upgrade package

Importing a software upgrade package

You can add customized FortiClient installation packages to the software upgrades list.

To import a package:

1. In the *FortiClient Manager*, go to *Manage* > *FortiClient Upgrade* and select Import.
2. Enter the *Version*, 4.0.3, for example.
3. Enter a *Description* of the package.

   This is important if you provide multiple custom installer packages.

4. From the *Platform* list, select the appropriate operating system type (32-bit or 64-bit Windows) for the package you will upload.
5. Select *Browse*, find the customized FortiClient installation file, and select *Open*.
6. Select *OK*.

   The file is uploaded and added to the FortiClient Software Upgrade list.

Deploying a software upgrade to clients

When you have downloaded FortiClient software upgrades to the FortiManager unit (see "Working with FortiClient software upgrades"), you can then deploy them to FortiClient agents.

To deploy software upgrades to FortiClient agents:

1. In the *FortiClient Manager*, select *Manage* > *FortiClient Upgrade* from the Main Menu Bar.
2. Select the *Deploy* icon for the software upgrade that you want to deploy.
3. Select whether to deploy the software to groups or to individual FortiClient agents. The options are
   - selected groups
   - selected groups and child groups
   - selected FortiClient agents
4. Enable *Select All* or select the particular groups or agents to receive the software upgrade.
5. Select *Apply*.

If an error occurs when upgrading a FortiClient agent's software, an alert is raised. See "Viewing upgrade alerts for FortiClient agents" on page 294.

FortiClient license keys

You can assign and deploy Premium (Volume) license keys to client groups. In the *FortiClient Manager*, go to *Manage* > *FortiClient Key* to view the current list of assigned license keys.

The FortiClient License Key Management page does not handle enterprise redistributable licensing. For information about using enterprise licensing, see "Configuring enterprise license management" on page 319.

There are several ways to apply Premium (Volume) licensing:

- Provide the license key to your users to enter directly into the FortiClient application. The license will by managed by FDS, not by FortiManager.
- Create a customized FortiClient installer that includes the license key. Distribute the customized FortiClient installer to your users. Use the "-a", and "-k" switches in the FCRepackager tool. For more information, see the *FortiClient Administration Guide*.
- If you manage FortiClient agent with a FortiManager unit, you can deploy the licenses. See "To deploy Premium (Volume) license with FortiManager:". The license is applied to all of your managed FortiClient agents that already do not have a Premium license. The volume license has a seat limit which the FortiManager unit enforces.

To deploy Premium (Volume) license with FortiManager:

1. Using *FortiClient Manager*, organize the managed FortiClient agent into client groups where all members use the same license key.
2. In the *FortiClient Manager*, go to *Manage* > *FortiClient Key* and select *Add* to add a license key to the FortiManager database.

3. In the *License Key* field, enter the license key.
4. Optionally, enter a description.
5. In the *Available Group(s)* list, select the client groups that use this license key and then select the green right arrow button to move the selected groups to the *Assigned Group(s)* list.
6. Click *OK*.
7. In the FortiClient *License Key Management* list, select the *Deploy to group* icon for the license key that you added. Click *OK* to confirm your request to deploy.

Working with web filter profiles

You can create web filter profiles in FortiManager and deploy them to FortiClient agents, FortiClient groups, Windows AD users, and Windows AD groups.

To assign web filter profiles to FortiClient agents and groups, see "Selecting a web filter profile for a FortiClient agent" on page 350.

To assign web filter profiles to Windows network users and groups, see "Working with Windows AD users and groups" on page 315.

About web filtering

FortiGuard web filtering is a managed Web Filtering solution provided by Fortinet. FortiGuard Web Filtering sorts hundreds of millions of web pages into a wide range of categories that users can allow, block, or monitor.

FortiGuard Web Filtering can also assign one of several classifications to denote web sites that provide cached content, such as web site search engines, or web sites that allow image, audio, or video searches.

The FortiClient agent accesses the nearest FortiGuard Web Service Point to determine the categories and classification of a requested web page. The FortiClient application blocks the web page if the web page is in a category or classification that is blocked in the assigned web profile.

There three predefined profiles to allow or block different combinations of web categories:

Default	Default web filter profile, which is initially the same as the child profile.
Child	Blocks categories that are not suitable for children.
Adult	Only blocks the security violating web sites.

You cannot delete the predefined profiles, but you can modify them. You can also create additional web profiles as needed.

You can assign web profiles to FortiClient agents and FortiClient groups. On a Windows AD network, you can also assign web profiles to each network user. *FortiClient Manager* sends the user's web filter information to the FortiClient agent where the user is logged on.

Viewing and editing web filter profiles

In the *FortiClient Manager*, go to *Global Configuration* > *Web Filter Profile* to manage web filter profiles.

Create New	Create a new web filter profile. See "Configuring a web filter profile" on page 310.
Name	The profile name
Comments	A description or comment about the profile
Action	
Delete icon	Delete this profile. You cannot delete the predefined Default, Child or Adult profiles.
Edit icon	Edit this profile.

Configuring a web filter profile

In the *FortiClient Manager*, go to *Global Configuration* > *Web Filter Profile*. Select *Create New* to create a new profile or select the *Edit* icon of an existing profile to modify the profile.

Enter the following information and select *OK*.

Name	Enter a name for the profile.
Comments	Optionally, enter descriptive information about the profile.
Bypass URLs **Block URLs**	Bypass URLs are allowed even if they are in a blocked category. Block URLs are always blocked. To add a URL, enter it in the field below the list and select *Add*. To remove a URL, select it in the list and then select *Delete*.
Select category to block	Either select *Select All* or select individual categories to block. You can expand the categories to select specific sub-categories.
Select classification to block	Either select *Select All* or select individual classifications to block.

Configuring FortiClient manager system settings

The *FortiClient Manager* system settings include:

- FortiClient configuration lockdown settings
- FortiClient agent discovery settings

FortiClient group administrators can only view these settings. For more information about group administrators, see "Configuring FortiClient group-based administration" on page 318.

In the *FortiClient Manager*, go to *Settings* > *System* > *System Setting*. Enter the following information and then select *Apply*.

FortiClient Lockdown	You can lock the configuration of FortiClient agents. Users cannot remove the software and cannot change the settings. Users can connect and disconnect VPN tunnels and can change certificates and CRLs. You can override the lockdown setting on groups or individual FortiClient agents. See "Configuring system settings of a FortiClient agent" on page 323.
Default policy for new client	Select *Enable Lockdown* or *Disable Lockdown*.
Lockdown password	Enter a password. You can provide this password to users to enable them to modify their own configuration, using FortiClient override. For information on the FortiClient override feature, see *FortiClient Endpoint Security User Guide.*
Apply Lockdown Setting to All	Apply the lockdown settings to all FortiClient agents that this FortiManager unit manages.
Client Discovery	
Accept client request	Select the network interfaces (ports) on which the FortiManager unit listens for registration requests, either broadcast or unicast, from FortiClient computers.
When new client is discovered	Select *Auto-populate managed client list* if you want newly-discovered FortiClient agents added to the Managed Client and Ungrouped Client lists in the navigation pane. Otherwise, select *Add to temporary client list*.
Other Setting	
Do retrieve configuration from client	Select to retrieve the configuration from a new client when it is added to the managed clients list.
Don't search static group and its child group(s)	Enable only to speed up dynamic grouping where there are no static groups with dynamic child groups. The default is to not enable this option.
Keep monitor alerts duration	Enter the time that firewall and antivirus alerts are retained before automatic deletion. Enter 0 to keep alerts until you manually delete them.
Keep management Event Logging duration	Enter the number of days to retain management event logs.

Configuring FortiClient manager clustering

Clustering enables you to support a large number of FortiClient agents by using multiple FortiManager units. One FortiManager unit must be declared as the primary unit. The others are all secondary units. For more information, see "About FortiClient Manager clustering" on page 286.

In the *FortiClient Manager*, go to *Settings* > *System* > *Cluster Setting* to configure *FortiClient Manager* clustering.

Enable cluster	Select to enable clustering and then enable one of the following options.
Cluster Run as Primary	Enable if this FortiManager is the primary unit. Select *Manage Secondary* to register secondary units. See "Configuring FortiClient manager cluster members" on page 312.
Cluster Run as Secondary	Enable if this FortiManager is a secondary unit. Enter address of the primary unit in the *Primary IP Address* field.

Configuring FortiClient manager cluster members

If you enable *FortiClient Manager* clustering and you set this FortiManager unit as the primary unit, you must register the other FortiManager units that are permitted to connect as secondary cluster members.

In the *FortiClient Manager*, go to *Settings* > *System* > *Cluster Setting* and select *Manage Secondary* to view or modify the list of secondary FortiManager units. Select *Return* when you are finished.

Register New	Select to add another secondary unit to the cluster. Enter the secondary FortiManager unit serial number and IP Address and then select *OK*. **Note:** If the secondary FortiManager is an HA cluster, enter the serial numbers of both units, separated by a comma.
FortiManager serial number	The serial number(s) of the secondary unit(s). You can find this information on the each secondary unit's *System Settings* > *General* page.
IP Address	The secondary unit's IP Address.
Enable	*Yes* or *No*
Connection	*Online* or *Offline*
Action	
Delete icon	Remove secondary unit from cluster.
Edit icon	Edit the secondary unit's information.

Configuring email alerts

You can configure *FortiClient Manager* to send email messages to administrators, or other parties, when there are management alerts or management events.

The *FortiClient Manager* sends an alert email message each day that there is a new alert or event. The email message contains all existing management alerts, and the total count of alerts. Optionally, the message can also contain the latest management events and total count of existing events.

In *FortiClient Manager*, go to *Settings* > *System* > *Email Alert Setting* to configure email alerts. Enter the following information and select *Apply*.

Enable Email alert	Send email alerts using the account and content settings below.
Email Account	
SMTP Server	Enter the SMTP mail server IP address or fully qualified domain name.
Port	Enter the port number that the mail server uses. The default is 25.
User authentication	Select if the mail server requires authentication, then enter the *Username* and *Password* of the sending email account.
Send to Administrator	
Administrator's Email address	Enter the email address of the person who will receive alerts.
Sender's Email address	Enter the reply-to address to provide in alert email messages.
Management Alert	Select if this email is in regards to a management alert.
Management Event	Select if this email is in regards to a management event.
Send test mail	Send a test email using the *Email Account* settings.
License notification	
Send alert email for enterprise client license	Select if the email is to notify to user of the FortiClient license.
Sender's email address	Enter the email address.

Configuring LDAP for web filtering

The FortiManager system can provide individualized web filter settings for users and groups on a Microsoft® Windows Active Directory network. A user can log on at any computer in the network. The FortiClient application on that computer requests web filter settings for that user from FortiManager.

In the *FortiClient Manager*, you assign web filter profiles to Active Directory (AD) groups and users. Users to which you have not assigned a profile are assigned to a default profile.

Configuring LDAP settings

FortiClient Manager uses LDAP protocol to retrieve information about Windows Active Directory users and groups from the domain controller.

In the *FortiClient Manager*, go to *Settings* > *LDAP Group/User* > *LDAP Settings* to view the list of LDAP servers.

Create New	Add another LDAP server. See "Configuring an LDAP server" on page 314.
Name	The name of the LDAP server.
LDAP Server	The server IP address and port of the Windows AD domain controller.
BaseDN	The Base Distinguished Name for the server. This describes what portion of the users and groups are in this server's database.
BindDN	The Distinguished Name the FortiManager must use to log on to the LDAP server to make queries. (Maximum 255 characters)
Action	
Delete icon	Delete this entry.
Edit icon	Modify the settings for this LDAP server. See "Configuring an LDAP server" on page 314.

Configuring an LDAP server

In the *FortiClient Manager*, go to *Settings* > *LDAP Group/User* > *LDAP Settings* and select *Create New* to add an LDAP server. You can also select the *Edit* icon for an LDAP server on the LDAP Settings page to modify the settings for an existing server.

Enter the following information and select *OK*.

Name	Enter a name for this LDAP server.
Server Name/IP	Enter the fully-qualified domain name or IP address of the Windows AD domain controller.
Server Port	Enter the port used to communicate with the LDAP server. The default is port 389. If needed, change the port to match the server.
BaseDN	Enter the Base Distinguished Name for the server. You can get this information from the server's administrator.
BindDN	Enter the Bind Distinguished Name for the server. You can get this information from the server's administrator.
Password	Enter the password required for logon to make queries.
Test Connection	Attempt to connect to LDAP server as configured. Results display below button.

Working with Windows AD users and groups

In the *FortiClient Manager*, go to *Settings* > *LDAP Group/User* > *LDAP Group/User* to view a list of Windows Active Directory (AD) domains, groups and users. You can assign web filter profiles to groups and users.

LDAP Groups view	
LDAP Users	Switch to LDAP Users view.
LDAP Server	Select the Windows Active Directory (AD) domain controller.
Synchronize	Update displayed group information from Windows AD server.
Domain	Windows AD domain. Expand domains to show groups. Each group names is preceded by a check box that you can use to select the group when assigning profiles. Select the group name to view group members.
Web Filter Profile	The web filter profile assigned to this group. To configure web filter profiles, see "Working with web filter profiles" on page 309.
Assign Profile / Web Filter Profile	Select a profile from the *Web Filter Profile* list and then select *Assign Profile* to assign it to the selected groups.

LDAP Users view	
LDAP Groups	Switch to LDAP Groups view.
LDAP Server	Select the Windows AD domain controller.
Synchronize	Update displayed user information from Windows AD server.
View	Select the number of users to list per page.
Line	Select the line of the list you want to view and press Enter.
First Page icon	Go to first page.
Previous Page icon	Go to previous page.
Next Page icon	Go to next page.
Last page icon	Go to last page.
Domain	Windows AD domain. Expand domains to show groups. Each group names is preceded by a check box that you can use to select the group when assigning profiles.
User Name / Go button	Find a name in the list. Enter the name and select Go.
Check box	Use the check box to select the user for web filter profile assignment. The check box in the table heading selects all users.
User Name	User name retrieved from Windows AD

Domain	Windows AD domain name
LDAP Server	Windows AD domain controller
Web Filter Profile	The web filter profile assigned to this user. To configure web filter profiles, see "Working with web filter profiles" on page 309.
Action	*Edit* icon - View information about this user.
Assign Profile / Web Filter Profile	Assign the profile selected in web filter profile list to the selected users.

Active Directory Organizational Units grouping

In a Microsoft® Windows server environment, a useful type of directory object contained within domains is the organizational unit. Organizational units (OU) are Active Directory (AD) containers into which you can place users, groups, computers, and other organizational units. An organizational unit cannot contain objects from other domains.

FortiClient Manager allows for AD OU grouping in order to easily manage FortiClient/AD OU groups. After you synchronize the AD server to *FortiClient Manager*, all the AD OUs are imported into *FortiClient Manager*. You can then keep all the policies set on a FortiClient group up to date, even when new FortiClient users are added to AD OUs.

After a new user is added to a AD OU group and FortiClient is installed on the user's computer, FortiClient automatically registers with *FortiClient Manager*. Then *FortiClient Manager* automatically places the new user into the correct group based on the computer's domain and computer name. After registration, *FortiClient Manager* sends the policies for the group the new user was placed in.

To add Active Directory Organizational Unit to FortiClient Manager groups:

1. Create the LDAP (Active Directory) server settings that will use the Organizational Units (OU). Go to *FortiClient Manager* > *Settings* > *LDAP Integration* > *LDAP Settings* and click *Create New*.
2. Configure the LDAP server settings. See "Configuring LDAP settings" on page 314.
3. Create the OU group. Go to *FortiClient Manager* > *Settings* > *LDAP Integration* > *AD OU Grouping* and click *Create New*.
4. In the *New AD Grouping* window enter the following information:

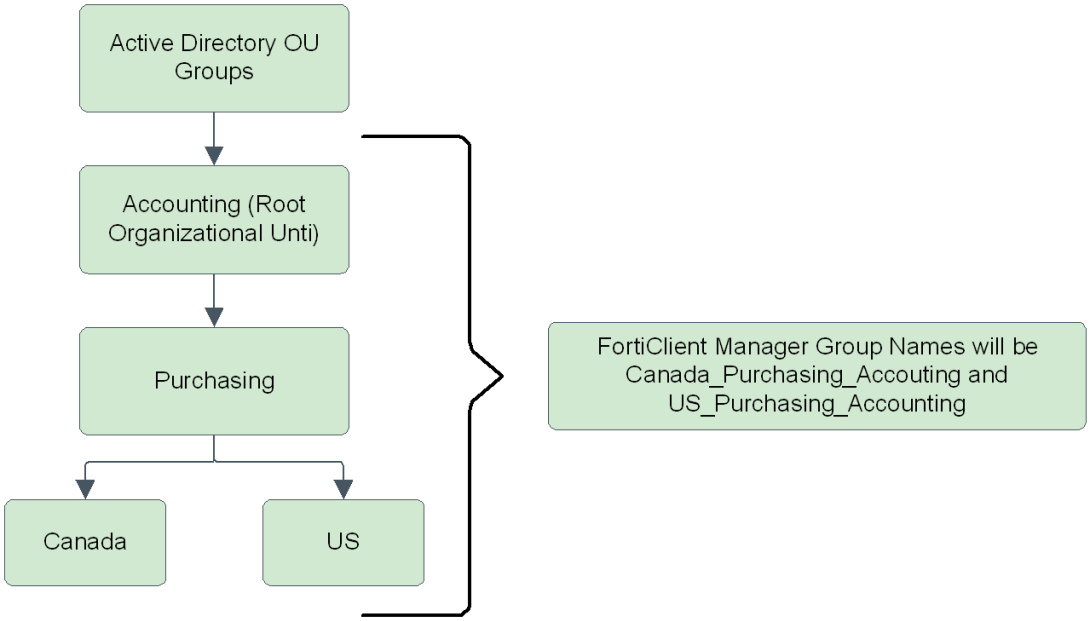
Name	Enter a name for the AD OU grouping.
LDAP Name	Select the name of the LDAP server created in Step 1.
Root OU	Select the OU group level. You can select any OU as the root OU. All OUs under the root OU will be imported into the FortiClient groups.
Description	Enter a description for the OU group.

5. Synchronize the AD OU and FortiClient. In the AD OU Grouping tab, click the *Synchronizing with AD Server* icon.
6. Once the synchronizing is complete, you can view the AD OU groups. Go to *FortiClient Manager* > *Client/Group* > *Group*. The OU groups are displayed in the tree.

   The imported FortiClient group names consist of the names of each level in the OU starting from the Root OU. For example, if the Root OU is Accounting and the subsequent level is

Purchasing, and then Canada and US at the same level, then the FortiClient group names will be Canada_Purchasing_Accounting and US_Purchasing_Accounting.

Figure 182: Example of how *FortiClient Manager* determines the group names for OU groups.



If an OU is deleted from the AD server, a delete icon is displayed on the group name in the tree and the word (Deleted) shown next to the group name to indicate that it has been deleted from the AD server. The FortiClient group name will remain in the list. You can copy its policy to another group and/or delete it from *FortiClient Manager* permanently.

7. Select the OU group from the tree to configure policies and browse FortiClient users. See "Configuring FortiClient agent settings" on page 321.

Synchronizing the AD server with FortiClient Manager

You can set the amount of time that *FortiClient Manager* automatically synchronizes with the Active Directory (AD) server to import any new or changed Organizational Units (OU) groups. The default time is 10 minutes.

After any new or changed OU groups are imported into *FortiClient Manager* and after FortiClient registers, *FortiClient Manager* matches the host name and domain name in the tree structure and puts it into the correct OU group. The policies on the OU group will be automatically pushed out to the new or changed clients.

To set the synchronize time:

1. Go to *FortiClient Manager* > *Settings* > *LDAP Integration* > *AD OU Grouping*.
2. Click *Settings*.
3. In the AD Group Settings tab, enter the number of minutes to synchronize the AD server with *FortiClient Manager*.
4. Click *Apply*.

Viewing the AD Grouping History

In the Active Directory (AD) Grouping History, you can see the Organizational Units (OUs) that have been added, deleted and the FortiClient group it belongs to when the AD server is synchronized with *FortiClient Manager*.

To view the AD Grouping history:

1. Go to *FortiClient Manager* > *Settings* > *LDAP Integration* > *AD OU Grouping*.
2. Click the *AD Grouping History* link.
3. In the *AD Grouping History* tab, you can search, delete or delete all the history.

Configuring FortiClient group-based administration

You can divide administration of FortiClient agent groups among several group administrators. A group administrator is assigned particular FortiClient groups and optionally also has access to ungrouped clients. With the assigned FortiClient agents, the group administrator can

- monitor status
- retrieve, modify and deploy configurations
- change group membership (among assigned groups only).

Any FortiManager administrator who does not have the Super_User administrator profile can become a *FortiClient Manager* group administrator. The permissions settings of the profile apply, except that FortiClient group administrators

- cannot modify *FortiClient Manager* global settings
- cannot create or edit FortiClient groups
- cannot delete a FortiClient agent
- cannot perform the Search/Add Client function or add a temporary client to the managed clients list
- cannot access clients that belong to another administrator's assigned groups
- cannot set the Roaming status of a FortiClient agent.

Assigning group administrators

In the *FortiClient Manager*, go to *Settings* > *Group Administration* to view the list of FortiClient group administrators. From this list, you can assign additional group administrators.

Add Assign	Select to assign client groups to administrators not already listed. See "To assign client groups to an administrator:".
Administrator	The group administrator.
Assigned groups	The client group(s) this administrator can manage.
Option	Shows "Allow access ungrouped client(s)" if that option is enabled. Otherwise, the field is blank.
Action	
Edit icon	Select to modify client group assignments or options for this administrator.
Delete icon	Select to delete the client group assignments for this administrator. This does not delete the administrator or the client groups.

To assign client groups to an administrator:

1. In the *FortiClient Manager*, go to *Settings* > *Group Administration* and select *Add Assign*.

   The *Edit Assigned Groups* page opens.

2. From the *Administrator* list, select the administrator.

   Only administrators who do not have the Super_User profile are available. The administrator must have read-write access to the *FortiClient Manager* configuration to modify FortiClient agent settings.
3. Optionally, select *Allow access ungrouped client(s)*.
4. In the *Available Groups* list, select the client groups that this administrator will manage and select the right-pointing arrow to move them to the *Selected Groups* list.
5. Select *OK*.

Configuring enterprise license management

With Enterprise (Redistributable) licensing, you obtain a re-distributable license from Customer Service & Support and subdivide that license into smaller "seat' licenses for your users. You can set the expiry date and seat count for each client license. The expiry date of your client licenses cannot be later than that of the enterprise license. The total seat count limit of your client licenses can exceed the seat count limit of the enterprise license, but the total number of managed clients cannot. FortiClient redistributable licensing can be validated by *FortiClient Manager* or by a company's own licensing validation system. For more information on internal validation, see the *FortiClient Administration Guide*.

The Redistributable license key can also be given to users and input into FortiClient manually.

To use enterprise licensing, you need to:

- Obtain an Enterprise License from Customer Service & Support and register it on your FortiManager unit.
- Create at least one enterprise client license for your FortiClient agent. See "Configuring an enterprise license" on page 319.
- Create a custom FortiClient installer that enables enterprise licensing. You can include the client license key in the installer or provide the client license key to users to apply after installation. The FortiClient application must be specifically customized for use with re-distributable licensing. You can use the FCRepackager tool to create a customized installer package that includes the redistributable license. Use the "-a", "-e" and "-k" switches. For more information, see the *FortiClient Administration Guide* and the *FCRepackager Read-Me* file.
- Deploy the customized FortiClient installer to your users.

Configuring an enterprise license

In the *FortiClient Manager*, go to *Settings* > *Enterprise License* to configure enterprise licensing. Enter the following information and select *Apply*.

	Enable License Management	Select the check box to use the FortiManager unit to manage licensing of FortiClient agents.
	Enterprise License Key	Enter the license key purchased from your Fortinet partner. Select *Download* to register the license. Information about the license appears below this field.
Validation Type		This section is available only if you downloaded a redistributable license.
	Internal Validation	Use the FortiManager unit to validate FortiClient license keys.

Enterprise Client License Management	Select this link to create enterprise client license keys for your FortiClient agents. For more information, see “Creating an enterprise client license key” on page 320.
External Validation	Use an external license key validation service.
Test Connection	If you are using external validation, select this button to confirm that the FortiManager unit can communicate with the external validation service.

Creating an enterprise client license key

After you register your enterprise license (see “Configuring an enterprise license” on page 319), you can create enterprise client licenses. For each of these licenses, you can set the expiry date and the seat limit. Client license expiry dates and the total number of seats licensed through enterprise client licenses cannot exceed the limits of the enterprise license.

To create enterprise client license keys:

1. Go to *Settings* > *Enterprise License* to configure the enterprise license.

   For more information, see “Configuring an enterprise license” on page 319.
2. Select the *Enterprise Client License Management* link.

   The list of enterprise client licenses is displayed.
3. Select *Add*.

   The *New Client License* dialog opens, with an enterprise client license key value in place.
4. In the *Name* field, enter a name to identify the license.
5. In the *Seats Permitted* field, enter a number seats that is within the range shown at the right.

   The maximum number of seats allowed is the enterprise license limit minus the number of enterprise client licenses actually issued to FortiClient agents.

   The total seats permitted in all enterprise client licenses can exceed the enterprise client limit. The FortiManager unit enforces the enterprise license limit only on the actual number of managed enterprise-client licensed FortiClient agents.
6. In the *Expiry Date* field, enter a date that is no later than that of the enterprise license.
7. Optionally, enter a description.
8. Select *OK*.

Creating a customized FortiClient installer

An enterprise client license key is effective only on FortiClient installations that are customized to accept an enterprise license instead of a standard fixed license. For more information, see the *FortiClient Administration Guide*. Distributing the customized FortiClient installer

You can distribute the customized FortiClient installer in various ways:

- Put the installer on a file share. Users simply double-click the file to begin installation.
- On a Windows Advanced Server network, install the application on end users’ computers remotely. For more information, see “Installing FortiClient using Active Directory Server” in the Installation chapter of the *FortiClient Administration Guide*.

Configuring FortiClient agent settings

You can configure managed FortiClient agents individually or in groups. All the configuration changes are stored in the FortiManager database until they are installed on the FortiClient agents.

For information on installing configuration changes on FortiClient agents, see "Deploying FortiClient agent configurations" on page 306.

When a FortiClient agent is a member of a group, most of its configuration is inherited from the group. You can only change an inherited setting by first selecting the Override option for that part of the configuration. You can reapply the group settings by selecting Apply to All Members in the group configuration.

To configure an individual FortiClient agent:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.

   You can also select *Client/Group* > *Group*, then select the group to which the client belongs.
2. From the *Host Name* column of the list of clients, select the client you want to edit.

   From the FortiClient menu, select the part of the configuration you want to edit, *Firewall* > *Policy* for example.
3. Reconfigure the client as needed and then select *Apply*.

To configure a group of FortiClient agents:

1. In the *FortiClient Manager*, in the navigation pane, select *Client/Group* > *Group*.
2. From the *FortiClient Group* list, select the name of the group that you want to configure.
3. From the FortiClient menu, select the part of the configuration you want to edit, *Firewall* > *Policy* for example.
4. Reconfigure the settings for the group as needed and then select *Apply*.

   For more information about configuring groups of clients, see "Configuring settings for client groups" on page 304.

Viewing system status of a FortiClient agent

You can display the managed FortiClient agents and view a agent's detailed information.

To view detailed FortiClient agent system status information:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want from the *Host Name* column.
3. From the FortiClient menu, select *General* > *Status*.

Connection Status	Indicates if the FortiClient agent is connected to the FortiManager unit. Online means connected. Offline means disconnected.
AV Engine Version	Displays the FortiClient agent's antivirus engine version number and whether it is up-to-date.
AV Signature Version	Displays the FortiClient agent's antivirus definition version number and whether it is up-to-date.
Information	

Host Name	The name of the FortiClient agent.
Description	The description from the FortiManager database.
IP Address	The IP address of the FortiClient agent.
DNS Domain	The DNS domain for the computer.
Operating System	The FortiClient computer operating system.
Windows Workgroup	The Windows Workgroup, if applicable.
Version	The FortiClient software version on the computer.
Serial No	The serial number of the FortiClient computer.
Expiry Date	FortiClient software license expiry date.
Last Connection	The time and date when the FortiClient agent last connected to the FortiManager unit.
Membership of Group	Drop-down list shows the FortiClient group to which the agent belongs or Ungrouped. Optionally, you can select a different group.
Roaming and allow dynamically grouping	Enable roaming and dynamic grouping for the FortiClient agent. Roaming computers are dynamically grouped when they change IP address. *FortiClient Manager* sends the new group configuration to the FortiClient agent.
Alerts	Displays the total number of alerts on the FortiClient agent.
Virus Alerts	Displays the number of virus alerts on the FortiClient agent.
Firewall Alerts	Displays the number of firewall alerts on the FortiClient agent.
Configuration	
Status	Indicates if the configuration changes made on the FortiClient agent through the FortiManager unit have been installed on the FortiClient agent itself. • Synchronized: The changes are installed. • Configuration Pending: The changes are not installed. For information on installing configuration changes, see “Deploying FortiClient agent configurations” on page 306.
Pending Configuration Details	Displays the configuration changes made on the FortiClient agent through the FortiManager unit that have been installed on the FortiClient agent and those that have not been installed. • A green check mark following a configuration name means the changes are installed. • A gray cross mark following a configuration name means the changes are not yet installed.
Apply	Save the configuration changes.

Configuring system settings of a FortiClient agent

You can configure a FortiClient agent's settings. You can also inherit system settings from the group to which the agent belongs.

To configure FortiClient agent system settings:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want from the *Host Name* column.
3. From the FortiClient menu, select *General* > *System Setting*.

Base Setting	
Override	This option is visible only if the FortiClient agent belongs to a group. The FortiClient agent's configuration includes settings inherited from the group. Selecting override allows you to modify the inherited system settings on this FortiClient agent. Deselecting override means that you want to use the system settings inherited from the group to which the agent belongs. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Show FortiClient console when user starts Windows	If selected, the FortiClient program will automatically run when the FortiClient agent starts up.
Hide the tray icon	Select to hide the FortiClient icon in the system tray. It will be active after FortiClient is restarted.
The tray icon does not flash	Select to not have the tray icon flash during antivirus scanning.
Raise alerts to FortiManager	If selected, the FortiClient agent will send alert information to the FortiManager unit.
Activated features	Select the features to be activated in FortiClient. When selected, the features will appear in FortiClient and the feature's services will affect the system. When clear, the features will be removed from FortiClient and the feature's services will be completely inactive. When deactivated, the features should still be configurable from *FortiClient Manager* although the configuration will not have any affect on the device. If the feature was not installed by the MSI, then it is not possible to activate the feature. To use this effectively, the full FortiClient product needs to be installed. It is possible to repackage the MSI so that although the feature is installed and it is initially 'deactivated'.
The interval of heartbeat message sent to FortiManager	Enter the number of seconds (10-300)

Validation type	Select the license validation type: Standard or Enterprise.
Update Server Setting	
Retrieve update package from	Select the source of FDS updates (antivirus, web filter, email filtering): • public FortiGuard network • the FortiManager unit for this agent • another server that you specify
Failover Port	Enter a valid port number.
Connection Timeout	Enter the connection timeout (60-600) in seconds. The default is 60.
If connection to customer server fails, try public FortiGuard network	Select to use the FortiGuard network if your enterprise server fails.
Update Schedule	
Enable Schedule update	Select to enable the update schedule. Enter the Daily time in hour and minutes or the number of hours.
Proxy setting	
Enable proxy for	If internet access from the FortiClient agent is installed on is via a proxy server, FortiClient may need to be configured with the details of that proxy so that it can • Updates - obtain updates • Virus submission - Submit suspicious files for analysis • Online SCEP - Perform certificate operations with remote servers.
Proxy/ Type/ IP Address/ Port	Select the proxy type and enter the IP address and port number for the proxy server.
User, Password	Enter the user name and password for the proxy server.
FortiProxy Setting	
The highest port number the proxy should listen on	Enter the number of ports the server can bind to. It should bind to as many ports as it needs starting at the highest port number specified here. If you have other server service that requires a specific port be left open, you should set the highest port number for FortiProxy to be less than that port number.
Disable FTP proxy	Select to disable the FTP proxy. FortiProxy tests network connectivity by sending packets to a designated IP address.
Disable selftest	Select to disable self test and enter the IP address used to test the network availability.

Disable SMTP client comforting/ Disable POP3 client comforting/ Disable POP3 server comforting	Some email clients may expect response packets from the smtp/pop3 server quickly after the packet was sent. Because FortiProxy may cache the outgoing packets, and incoming server response until all the packets are scanned for malware/spam, the client application may throw a “response timeout” error. When client comforting is enabled, FortiProxy will "drip" packets to the client at a rate that is fast enough to stop the client from erroring, but slow enough to stop the entire response being sent to the client before the response from the server is fully scanned. Select the check boxes to disable these features.

Adding trusted FortiManager units to a FortiClient agent

When installing the FortiClient software, users must set up at least one trusted FortiManager unit. (For more information, see *FortiClient Software v4.0 Release Notes*.) Later, you can add more trusted FortiManager units through the *FortiClient Manager* and push them to the FortiClient agents. Then the FortiClient agents can be managed by the trusted FortiManager units.

Create New	Select to add a FortiManager unit to manage FortiClient agents.
Override	The FortiClient agent’s configuration includes those inherited from the group to which the agent belongs. Selecting override allows you to modify the inherited trusted FortiManager configuration on this FortiClient agent. Deselecting override means that you want to use the trusted FortiManager configuration inherited from the group to which the computer belongs. Even with inherited trusted FortiManager configurations, you can still add new trusted FortiManager units for a FortiClient agent. See “Adding a FortiClient agent group” on page 302 and “Configuring settings for client groups” on page 304.
Name	Name of a trusted FortiManager unit.
Trusted FortiManager	IP address/range of a trusted FortiManager unit.
Comments	Any notes for a trusted FortiManager unit.
Action	Select the Delete icon to remove a trusted FortiManager unit, and the Edit icon to modify the values of a trusted FortiManager unit. When configuring a group, to copy the trusted FortiManager definition to other groups select Copy to other group.

To add a trusted FortiManager unit:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want from the *Host Name* column.
3. From the FortiClient menu, select *General* > *Trusted FortiManager*.
4. Select *Create New*.

5. In the *Name* field, enter a unique name for the trusted FortiManager unit.
6. From the *Type* list, select the type of address information you have for the trusted FortiManager unit and enter it in the field.
   - **Single Address:** the IP address of the unit.
   - **IP Range**: the IP range that includes the unit.
   - **Subnet:** the IP address and network mask of the subnet that includes the unit.
   - **FQDN**: the fully qualified domain name of the unit.
7. Optionally, add information about the unit in the *Comments* field.
8. Select *OK*.

Managing pending actions for a FortiClient agent

The Pending Action page displays the action items to be executed on the selected FortiClient agent by the FortiManager unit. The queue appears when the action items cannot be executed instantly due to reasons such as the FortiClient agents are offline or behind firewalls. It disappears when the actions are successfully completed. The action items include:

- Install configuration: install configuration changes to a FortiClient agent. See "Deploying FortiClient agent configurations" on page 306.
- Retrieve configuration: resynchronize with a FortiClient agent by pulling the FortiClient configurations from the computer and save it to the FortiManager database. See "Retrieving a FortiClient agent configuration" on page 306.
- Notify AV engine/database upgrading: a FortiClient agent's antivirus engine/database expires.
- Change lockdown configuration: enable or disable lockdown on a FortiClient agent. See "Configuring lockdown settings" on page 328.

To display the pending actions of a FortiClient agent:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want from the *Host Name* column.
3. From the FortiClient menu, select *General* > *Pending Action*.

View Per Page	Select the maximum number of actions to display per page.
Page controls	Go to the first, previous, next or last page of the list.
Action	The action items to be executed.
Information	The most up-to-date AV Signature/AV engine version numbers on the FortiManager unit. This information only applies to the Notify AV engine/database upgrading action.
Time	When the action was initiated.
Action	Delete icon - Deletes the action item manually.
Delete	Delete the selected pending actions.
Delete All	Delete all pending actions.

Configuring the log settings of a FortiClient agent

You can configure logging of different types of events for any or all of the FortiClient services by specifying the log level, log type, log size, and log entry lifetime.

To configure log settings:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *General* > *Log Setting*.
4. Configure the following settings and select Apply.

Override	The FortiClient agent's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited remote log settings on this FortiClient agent. Deselecting override means that you want to use the remote log settings inherited from the group to which the computer belongs. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Remote Server	Select to save the logs to a remote FortiAnalyzer or syslog server.
Server type	Select *FortiAnalyzer* or *SysLog* as required.
Hostname/IP	Enter the FQDN or IP address of the logging server.
Facility	Select the Facility setting as required. Facility is one of the information fields associated with a log message. If each FortiClient installation is configured to use a different facility setting, you can easily determine the source of a FortiClient log message.
Log level	Select the minimum severity of message to be logged. You can select *Error*, *Warning* or *Information*. The default is *Warning*.
Local (Disk)	These settings apply to logging on the FortiClient agent.
Log file size (max)	Enter the maximum space allocated to FortiClient logs. The default is 5120 KB. Log entries are overwritten, starting with the oldest, when the maximum log file size is reached.
Log level	Select the minimum severity of message to be logged. You can select *Error*, *Warning* or *Information*. The default is *Warning*.
Enable Custom Field	Enable the following custom log field to be included in all logs from this FortiClient agent. This field can be used in generating reports on the FortiAnalyzer unit.
Name	Enter the name of the custom log field.
Value	Enter the value of the log field.

5. Select *Apply*.

Configuring lockdown settings

When lockdown is enabled, all configuration on the selected FortiClient agent will be read-only at the computer. Users cannot remove the software and cannot change the settings. However, users can connect and disconnect VPN tunnels and can change certificates and CRLs.

If you want to allow the FortiClient user to modify the configuration, you can set the lockdown password and send it to the user who can then use the FortiClient override feature to unlock the configuration.

For global FortiClient lockdown settings, see "Configuring FortiClient manager system settings" on page 310.

To configure lockdown settings:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *General* > *Lockdown*.
4. Select the *Settings are inherited from group* check box to inherit the settings from the group.
5. Select the *Enable Lockdown* check box.
6. Enter the password and click *Apply Lockdown*.

Configuring the VPN settings of a FortiClient agent

The *FortiClient Manager* can automatically download a VPN setting from the FortiGate unit running FortiOS v4.0 or higher to which your FortiClient agent connects.

If the VPN gateway that your FortiClient agent connects to is a third-party gateway, you must configure the FortiClient VPN settings on the FortiClient agent manually.

If the agent is locked down by *FortiClient Manager*, you cannot change the VPN configuration. However, you can connect or disconnect VPN tunnels that are already configured. Lockdown can be applied globally (see "Configuring FortiClient manager system settings" on page 310) or on specific FortiClient agents (see"Configuring system settings of a FortiClient agent" on page 323).

Create New	Select to create a VPN.
Override	The FortiClient agent's configuration includes those inherited from the group to which the agent belongs. Selecting override allows you to modify the inherited VPN policy on this FortiClient agent. Deselecting override means that you want to use the VPN policy inherited from the group to which the agent belongs. Even with inherited VPN policies, you can still create new VPN policies for a FortiClient agent. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Name	The name for the VPN.
Type	The type of methods used to create VPNs. In this release, only the automatic method is supported.

Policy Server	The IP address of the VPN gateway, that is, the FortiGate unit running FortiOS v4.0 that the FortiClient agent connects to.
Action	Select the Delete icon to remove a VPN, and Edit icon to modify a VPN. Select Copy to Group to add this configuration to the group to which this FortiClient agent belongs.

To configure VPN settings:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *VPN* > *Download Connection*.
4. Select *Create New*.
5. Enter a descriptive name for the VPN connection.
6. For *Category*, select *Automatic*.
7. For *Policy Server*, enter the IP address of the VPN gateway.
8. Select *OK*.

Configuring a VPN security policy on a FortiClient agent

For enhanced network security, you can require the FortiClient agent to have security features active before it initiates a VPN connection.

To configure a VPN security policy:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *VPN* > *Security Policy*.
4. Select any of the following policies that you want to enforce:
   - Firewall must be enabled
   - Real time AV must be enabled
   - Web filtering must be enabled
   - Email filtering must be enabled
5. Select *Apply*.

Configuring VPN options of a FortiClient agent

Set the VPN options for computers running FortiClient.

To set the VPN options:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *VPN* > *VPN Option*.

4. Select *Start VPN before logging on to Windows* if you need to log on to a Windows domain through a VPN when you start up your Windows workstation.
5. Select *Keep IPsec service running forever unless manually stopped* to retry dropped connections indefinitely. By default, the FortiClient software retries a dropped connection four times.
6. Select *Beep when connection error occurs* if you want the FortiClient software to sound a beep when a VPN connection drops. By default, the alarm stops after 60 seconds, even if the connection has not been restored. You can change the duration or select *Continuously* so that the alarm stops only when the connection is restored.
7. Select *Allow remember credentials* to allow eXtended Authentication VPN credentials for a tunnel to be remembered and automatically used the next time the user tries to connect to the VPN tunnel. See the *FortiClient Endpoint Security Guide* for more information on eXtended Authentication.

Configuring WAN Optimization settings of a FortiClient agent

FortiClient WAN Optimization can work together with WAN Optimization on a FortiGate unit to accelerate network access. FortiClient will automatically detect if WAN Optimization is enabled on the optimizing remote gateway it is connected to and transparently make use of the data reduction and compression features available. Data reduction and compression are bidirectional.

Override	The FortiClient agent's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited trusted FortiManager configuration on this FortiClient agent. Deselecting override means that you want to use the trusted FortiManager configuration inherited from the group to which the computer belongs. Even with inherited trusted FortiManager configurations, you can still add new trusted FortiManager units for a FortiClient agent. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Enable WAN Optimization	Enable the WAN Optimization feature. Configure the following options.
Optimize for	Select the protocols to optimize: HTTP, CIFS, MAPI, FTP
Maximum disk cache size	Set maximum disk cache size. Range is 256 to 32 768 MBytes. Entry is rounded to nearest 64MBytes (values 256, 320, 384, and so on). If your hard disk can accommodate a larger cache, better optimization performance is possible.

To enable WAN optimization:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want from the *Host Name* column.
3. From the FortiClient menu, select *WAN Optimization* > *Settings*.
4. Select *Enable WAN Optimization*.
5. Enable the protocols to be optimized: *HTTP* (web browsing), *CIFS* (file sharing), *MAPI* (Microsoft Exchange) and *FTP* (file transfers).

6. Set *Maximum Disk Cache* to 512, 1024, or 2048MB.

   The default is 256MB. If your hard disk can accommodate a larger cache, better optimization performance is possible.
7. Select *Apply*.

Configuring antivirus settings on a FortiClient agent

The antivirus feature allows you to protect your computer by regularly scanning the computer for viruses. You can also configure real-time virus protection.

To view antivirus alerts:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Antivirus* > *Alert* to view the viruses found on the selected computer.

Find Virus/Filename	Enter the name of a virus and select Go to search for it.
Delete All	Select to delete all virus alerts.
#	The virus identifier. Viruses are numbered in the order they are found.
Time	The time when the virus was found.
Virus	The name of the virus.
Filename	The virus-infected files

To view virus scan schedules:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Antivirus* > *Scheduled Scan*.

Create New	Select to create a virus scan schedule.
Override	The FortiClient agent's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited virus scan schedule on this FortiClient agent. Deselecting override means that you want to use the virus scan schedule inherited from the group to which the computer belongs. Even with inherited virus scan schedules, you can still create new schedules for a FortiClient agent. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Name	Name of the virus scan schedule.

Type	Type of the virus scan schedule: daily, weekly, or one-time.
Scan Level	Indicates whether it is a basic scan or full scan.
Schedule	Timing of the scan. This value is set depending on the type of the virus scan schedule.
Action	Select the Delete icon to remove a virus scan schedule, and Edit icon to modify a virus scan schedule.

To schedule a virus scan:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Antivirus* > *Scheduled Scan*.
4. Select *Create New*.
5. Configure the following settings and then select *OK*.

Name	Enter a name for the scheduled scan.
Scan Level	Select a scan level: basic or full scan.
Type	Select the scan frequency. The fields change depending on the type you select. Enter the time, date, and year for the scan accordingly.
Scan Time	Select the scan starting time.

Antivirus scans

The antivirus scan feature enables *FortiClient Manager* to request FortiClient to perform scans immediately on the target drives and directories specified.

If FortiClient alerts *FortiClient Manager* if any viruses or malware is found. Virus alerts are visible in the *Message Center* > *Client Alert*.

To do a quick scan:

A quick scan scans “in memory” processes and malware using the malware detection engine.

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Antivirus* > *Scan*.
4. Click *Quick Scan*.

   The antivirus alert page is shown with the list of infected files. See “Viewing antivirus alerts for FortiClient agents” on page 294.

To do a full system scan:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Antivirus* > *Scan*.
4. Select *Network drives* or *Removable media* if you want them included in the scan.
5. Select the relative priority of virus scanning compared to other processes
6. Click *Quick Scan*.

   The Antivirus Alert page is shown with the list of infected files. See "Viewing antivirus alerts for FortiClient agents" on page 294.

To do a directory scan:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Antivirus* > *Scan*.
4. Select one of the following:
   - Scan drive — Enter the drive letter to scan.
   - Scan the drive that the Windows is installed on
   - Scan "Program Files" folder
   - Scan "Windows" folder
   - Scan "Documents and Settings" folder
5. Click *Directory Scan*.

Configuring antivirus options

You can configure the following antivirus options:

- Email scan options
- Real-time protection options
- Scheduled scan options
- Server protection options
- Quarantine options

Email scan options

You can scan incoming and outgoing email messages and email attachments for viruses and worms.

To configure an email scan:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *AntiVirus* > *Option* > *Email Scan*.

4. Configure the following settings:

Override	The FortiClient agent's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited email scan configuration on this FortiClient agent. Deselecting override means that you want to use the email scan configuration inherited from the group to which the computer belongs. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Enable e-mail scanning	Select to activate email scanning.
Enable worm detection (Email client)	Select to prevent worms from spreading with emails.
Enable heuristic scan of attachments	Select to scan email attachments to find the unknown viruses and threats that have not yet been cataloged with signatures.
Virus or suspicious email action	*Log/Alert Only:* display a message if a virus is detected during real-time file system monitoring. *Strip & Quarantine:* move the file to a quarantine directory.

Real-time protection options

Configure the real-time protection settings to specify what types of files to scan and exclude and what happens when a virus is detected during real-time system monitoring.

To configure real-time protection:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *AntiVirus* > *Option* > *Real-time Protection*.
4. Configure the following settings.

Override	The FortiClient agent's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited realtime protection configuration on this FortiClient agent. Deselecting override means that you want to use the realtime protection configuration inherited from the group to which the computer belongs. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Enable Real-time Protection	Select to activate real-time protection.

Monitoring startup program list	Select to enable FortiClient to monitor changes to the list of programs that are started automatically when the computer starts.
Virus found action	Select the action FortiClient takes when a virus is found: *Deny Access*: Do not allow user to open, run or modify the file until it is cleaned. *Quarantine:* Move the file to a quarantine directory. *Clean*: Attempt to remove the virus from the infected file. If this is not possible, quarantine the file.
File type exempt list	Use Add to enter the file types that you do not want to scan. Use Delete to remove file types.
File exempt list	Use Add to enter specific files that you do not want to scan. Use Delete to remove files from the list.
Folder exempt list	Use Add to enter the folders that you do not want to scan. Use Delete to remove folders.
Advanced	Optionally, you can: • specify whether to scan compressed files and the file size limit. The default size limit is 0, which means no limit. • specify whether to scan several types of grayware. • enable heuristic scanning. FortiClient software uses heuristic techniques to scan files to find the unknown viruses and threats that have not yet been cataloged with signatures. Heuristics looks at characteristics of a file, such as size or architecture, as well as behaviors of its code to determine the likelihood of an infection. • enable scanning when reading or writing to disk. • enable scanning of network drives.

5. Select *Apply*.

Scheduled scan options

You can set the options for when FortiClient performs a scheduled scan.

To set scheduled scan options:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *AntiVirus* > *Option* > *Scheduled Scan*.

4. Configure the following options and then select *Apply*.

Scheduled Scan	
Virus found action	Select one of the following: **Alert** - display a message **Quarantine** - move the file to quarantine **Clean** - attempt to remove the virus from the infected file. If this is not possible, move the file to quarantine.
Integrate with Windows shell	Add a FortiClient antivirus scan command to the Windows Explorer shortcut menu.
Notify when the virus signature is out of date	Although the FortiClient application can alert the user that the virus signature is outdated, if you manage AV updates centrally this notification might confuse users.
Scan removable media on insertion	Enable the FortiClient application to scan removable media, such as USB drives, automatically.
Pause AV scanning if computer switches to battery power or UPS	Enable to reduce drain on batteries by not scanning when the computer is on battery power.
Exempt List	
File type exempt list	This list specifies file types to not scan. To add a file type to the list, enter the file extension in the box and select Add. To remove a file type, select it in the list and then select Delete.
File exempt list	This is a list of specific files to not scan. To add a file to the list, enter the file path in the box and select Add. To remove a file, select it in the list and then select Delete.
Folder exempt list	This is a list of specific folders to not scan. To add a folder to the list, enter its path in the box and select Add. To remove a folder, select it in the list and then select Delete.
Virus Submission	
Use this email account to submit the virus	Instead of using the default mail server, you can specify an SMTP server to use when submitting the quarantined files.
SMTP server	Enter the SMTP server that is used for outgoing mail.
User authentication	If the SMTP server needs authentication to log on, select this check box.
User name	Enter the user name for the SMTP server.

Password	Enter the password for the SMTP server.
Enable automatically submitting suspicious files to Fortinet Inc.	Select to send any suspicious virus files to Fortinet.
File types to scan	
All files	Select to scan all files.
Program files and documents	If you do not want the FortiClient software to scan all files for viruses, select this option.
File types to scan	Enter the file types to scan for.
Files with no extension	Select to scan files that have no extension.
Advanced	
Scan Compressed Files	Scan compressed files, such as .zip files. Enter the maximum size of file to scan. The default size limit is 0, which means no limit.
Scan Grayware	Select the types of grayware that FortiClient looks for while scanning.
Enable Heuristic scanning	FortiClient software uses heuristic techniques to scan files to find unknown viruses and threats that have not yet been cataloged with signatures. Heuristics looks at characteristics of a file, such as size or architecture, as well as behaviors of its code to determine the likelihood of an infection.
AV signature	
Use small DB (Small DB is only supported by FortiClient v4.0)	If you only want to scan for active viruses, select the check box. The core signature database is comprised of viruses that are currently active. This option will take lesser time to scan your computer because of the smaller database. The core signature database does not require a license and is updated frequently.
Use Extended DB (Extended DB is supported by FortiClient 4.1 upwards)	Select the check box if you want to do antivirus scans using the full antivirus database. The extended signature database is comprised of the full antivirus database. Using this option will take a longer time to scan your computer. The extended signature database requires a premium license and is updated less frequently.

Server protection options

You can set the Microsoft Exchange and Microsoft SQL server settings options.

If Microsoft Exchange or SQL servers are installed, allowing antivirus to scan the product files can cause these products performance problems or cause product failure.

To set the server protection options:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *AntiVirus* > *Option* > *Server Protection*.
4. Configure the following options and then select *Apply*.

Exchange Server Setting	
Integrate virus scanning into Exchange 2003/2007	Select to scan Microsoft Exchange data stores for viruses.
What to do when a virus is found	• Quarantine the attachment — The message and attachment is quarantined. • Remove the attachment only — The infected attachment is removed, but the body of the message remains.
Exclude the Exchange filesystem files from scanning	Fortinet recommends that you enable this setting to avoid impairing the operation of the Exchange server.
SQL Server Setting	
Exclude SQL Server filesystem folders from virus scanning	Fortinet recommends that you enable this setting to avoid impairing the operation of SQL server.
Exclude all files that have extensions associated with SQL Server from virus scanning	Fortinet recommends that you enable this setting to avoid impairing the operation of SQL server.

Quarantine options

You are able to specify the number of days to retain the quarantined files. Quarantine retains all files until you delete or restore them, unless you configure automatic deletion.

To set the quarantine options:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *AntiVirus* > *Option* > *Quarantine*.
4. Select the *Delete files older than* check box and enter the number of days to retain files.
5. Click *Apply*.

Viewing the firewall monitor of a FortiClient agent

On the FortiClient agent, when an application tries to connect through the firewall, FortiClient Host Security normally prompts the user to allow or disallow the access unless there is a matching firewall policy. When controlled by FortiManager, the FortiClient application blocks all

access for which there is no firewall policy and raises a firewall policy violation alert to the FortiManager unit.

Optionally, you can change the FortiClient default to allow all accesses for which there is no Deny firewall policy. See “Setting the firewall options of a FortiClient agent” on page 348.

Based on the violations recorded in the firewall monitor, you can add new firewall policies to allow or disallow these access attempts in future.

Select a FortiClient agent in the All Managed Clients or Ungrouped Clients lists and open its Firewall Monitor. Firewall Monitor displays firewall policy violation events that occur on the managed FortiClient agents.

Source / Destination	The source and destination address to which the policy applies. See “Configuring firewall addresses on a FortiClient agent” on page 341.
Service / Port	Protocols of the connection attempts.
# Violations	The number of firewall policy violations.
Last Violation	The date and time of the most recent violation.
Action	
Delete icon	Select to delete a firewall violation record.
Edit icon	Select to create a policy for a firewall violation event if there is no existing policy for the event. See “To create a policy for a firewall violation event:” on page 339.
Delete	Delete the selected firewall violation records for this device.

To create a policy for a firewall violation event:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Firewall* > *Monitor*.
4. For the firewall violation event that you want to add a policy, select the *Edit* icon.

Destination	Create a new address name or select an existing one. If you create a new address name, this name is linked with this violation event. If you choose an existing address, it may not be linked to this violation event. See “Configuring firewall addresses on a FortiClient agent” on page 341.
Service	Create a new service or select an existing one. If you create a new service name, this name is linked with this violation event. If you choose an existing service, it may not be linked to this violation event. See “Defining firewall protocols on a FortiClient agent” on page 344.
Schedule	Select the schedule that controls when the policy should be active. See “Configuring firewall schedules on a FortiClient agent” on page 346.
Action	Select the response to make when the policy matches a connection attempt.
Comment	Optionally, add any comments you have for this policy.

5. Select *OK*.

Creating firewall policies on a FortiClient agent

Firewall policies are instructions that the FortiClient program uses to decide what to do with a connection request. When managed by a FortiManager unit, the FortiClient firewall operates in Custom Profile mode.

Create global firewall policies to control traffic generally. These policies create FortiClient advanced firewall rules.

Create application firewall policies to control specific applications' access to the network. These policies create FortiClient advanced application firewall rules.

Create New	Create a firewall policy.
Override	The FortiClient agent's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited firewall policy on this FortiClient agent. Deselecting override means that you want to use the firewall policy inherited from the group to which the computer belongs. Even with inherited firewall policies, you can still create new firewall policies for a FortiClient agent. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Name	The policy name.
Application	For an application policy, select the application. If the application is not listed, go to *Application* > *Application* in the FortiClient menu. See "Defining firewall applications on a FortiClient agent" on page 343.
Source	The source address to which the policy applies. See "Configuring firewall addresses on a FortiClient agent" on page 341.
Destination	The destination address to which the policy applies. See "Configuring firewall addresses on a FortiClient agent" on page 341.
Schedule	The schedule that controls when the policy should be active. See "Configuring firewall schedules on a FortiClient agent" on page 346.
Protocol	The service to which the policy applies. See "Defining firewall protocols on a FortiClient agent" on page 344.
Action	The response to make when the policy matches a connection attempt: *Allow* or *Block*.
Enable	Enable or disable the policy. Enabling the policy makes it available for the firewall to match it to incoming or outgoing connections.
Action	Select the Delete icon to remove a policy, and Edit icon to modify a policy.

To create a firewall policy:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.

2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select one of the following:
   - for a general firewall policy, *Firewall* > *Policy* > *Global Policy*
   - for an application-specific policy, *Firewall* > *Policy* > *Application Policy*
4. Select *Create New*.
5. Enter the field value as described above and then select *OK*.

Configuring firewall addresses on a FortiClient agent

Add, edit, and delete firewall addresses as required. Firewall policies specify firewall addresses to match the source or destination IP addresses of packets that the FortiClient agent receives.

Create New	Select to create a firewall address for the managed FortiClient agent.
Override	The FortiClient agent's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited firewall address configuration on this FortiClient agent. Deselecting override means that you want to use the firewall address configuration inherited from the group to which the computer belongs. Even with inherited firewall address configurations, you can still create new firewall addresses for a FortiClient agent. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Name	The name of the firewall address.
Type	Select one of *Single Address*, *IP Range*, *Subnet*, or *FQDN*.
Single Address **IP Range** **Subnet** **FQDN**	This name and format of this field depends on the *Type* setting. *Examples*: • Single Address: `10.10.1.2` • IP Range: `10.10.1.[12-20]` or `10.10.1.12-10.10.1.20` • Subnet: `10.10.10.0/255.255.0.0` • FQDN: `mysite.example.com`
Comments	Comments on the firewall address.
Action	*Delete:* Remove the selected firewall address. *Edit*: Modify the firewall address. *Copy to group:* If the FortiClient agent belongs to a client group, add this address to the group configuration.

To add a firewall address:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want from the *Host Name* column.
3. From the FortiClient menu, select *Firewall* > *IP Address* > *IP Address*.

4. Select *Create New*, enter the information as described above and then select *OK*.

Configuring firewall address groups on a FortiClient agent

You can create groups of firewall addresses for use in firewall policies. The default Address Groups are Blocked-Zone, Public-Zone, and Trusted-Zone. You can edit these Address Groups or create new groups.

Create New	Select to create a firewall address group.
Override	The FortiClient agent's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited firewall address group configuration on this FortiClient agent. Deselecting override means that you want to use the firewall address group configuration inherited from the group to which the computer belongs. Even with inherited firewall address group configurations, you can still create new firewall address groups for a FortiClient agent. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Name	The name of the firewall address group.
Member	The addresses in the address group.
Comments	Comments on the firewall address group.
Action	Select the Delete icon to remove a firewall address group, and Edit icon to modify a firewall address group.

To add a firewall address group:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want from the *Host Name* column.
3. From the FortiClient menu, select *Firewall* > *IP Address* > *Address Group* > *Create New*.

Group Name	Enter a name to identify the address group. You must not use the same name as any firewall address or virtual IP.
Comments	Optionally, add comments on the firewall address group.
Group Members	Use the arrows to move addresses between the *Available Address* (configured and default firewall addresses) and *Selected Address* lists. The list of addresses come from the IP Addresses.

4. Select *OK*.

Defining firewall applications on a FortiClient agent

Define applications so that you can create firewall policies to allow or deny network access to these applications. For information about creating firewall policies for applications, see "Creating firewall policies on a FortiClient agent" on page 340.

Create New	Select to create a firewall application.
Override	The FortiClient agent's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited firewall application configuration on this FortiClient agent. Deselecting override means that you want to use the firewall application configuration inherited from the group to which the computer belongs. Even with inherited firewall application configurations, you can still create new firewall applications for a FortiClient agent. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Name	The name of the firewall application.
Details	The information about the firewall application, including its executable file name, size, and checksum.
Comments	Comments on the firewall application.
Action	Select the *Delete* icon to remove a firewall application, and *Edit* icon to modify a firewall application.

To define a firewall application:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Firewall* > *Application* > *Create New*.

Name	Enter a name to identify the application.
Executable File	Enter the executable file name of application. For example, the executable of Internet Explorer is iexplorer.exe. Optionally you can leave this field blank to define the service only by its ports.
File size	Enter the size of the executable file. If *Executable File* is blank, enter a value that is not the same as that of any other application executable file.
Checksum (CRC32)	Enter the CRC32 checksum of the executable file. If *Executable File* is blank, enter a value that is not the same as that of any other application executable file. The checksum and file size are used to uniquely identify the application executable file.
Comments	Enter any comments on the firewall application.

4. Select *OK*.

Defining firewall protocols on a FortiClient agent

Define protocols so that you can create firewall policies to allow or deny use of these protocols. You define a protocol in terms of the UDP or TCP ports that it uses. See "To define a firewall protocol:" on page 344.

To make it easier to add policies, create groups of protocols and then add one policy to allow or block access for all the protocols in the group. A protocol group cannot be added to another protocol group. See "Configuring firewall protocol groups on a FortiClient agent" on page 345.

Create New	Select to create a firewall protocol.
Override	The FortiClient agent's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited firewall service configuration on this FortiClient agent. Deselecting override means that you want to use the firewall service configuration inherited from the group to which the computer belongs. Even with inherited firewall service configurations, you can still create new firewall services for a FortiClient agent. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Name	The name of the firewall protocol.
Type	The type of protocol: TCP, UDP, TCP/UDP or ICMP
Source Port	Source port for the protocol.
Destination Port	Destination port for the protocol.
Action	Select the Delete icon to remove a firewall protocol, and Edit icon to modify a firewall protocol.

To define a firewall protocol:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Firewall* > *Protocol* > *Create New*.

Name	Enter a name to identify the protocol.
Protocol	Select the protocol type: TCP, UDP, TCP/UDP or ICMP.
Source Port	Specify the source port number for the protocol. (Not for ICMP.)
Destination Port	Specify the destination port for the protocol. (Not for ICMP.)
Comments	Enter any comments on the firewall protocol.

4. Select *OK*.

Configuring firewall protocol groups on a FortiClient agent

You can create groups of firewall protocols for use in firewall policies.

Create New	Select to create a firewall protocol group.
Override	The FortiClient agent's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited firewall protocol group configuration on this FortiClient agent. Deselecting override means that you want to use the firewall protocol group configuration inherited from the group to which the computer belongs. Even with inherited firewall protocol group configurations, you can still create new firewall protocol groups for a FortiClient agent. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Name	The name of the firewall protocol group.
Member	The services added to the protocol group.
Comments	Comments on the firewall protocol group.
Action	Select the Delete icon to remove a firewall protocol group, and Edit icon to modify a firewall protocol group.

To create a firewall protocol group:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Firewall* > *Protocol* > *Protocol Group* > *Create New*.

Group Name	Enter a name to identify the protocol group.
Comments	Enter any comments on the firewall protocol group.
Available Protocols	The list of configured protocols. Use the arrows to move protocols between the lists.
Members	The list of protocols in the group. Use the arrows to move protocols between the lists.

4. Select *OK*.

Configuring firewall schedules on a FortiClient agent

Use recurring schedules to control when policies are active or inactive. Recurring schedules repeat weekly and are effective only at specified times of the day or on specified days of the week.

Create New	Select to create a firewall recurring schedule.
Override	The FortiClient agent's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited firewall schedule configuration on this FortiClient agent. Deselecting override means that you want to use the firewall schedule configuration inherited from the group to which the computer belongs. Even with inherited firewall service group configurations, you can still create new firewall schedules for a FortiClient agent. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Name	The name of the firewall schedule.
Day	The start day for the schedule.
Start	The start time for the schedule.
Stop	The stop time for the schedule.
Comments	Comments on the firewall schedule.
Action	Select the Delete icon to remove a firewall schedule, and Edit icon to modify a firewall schedule.

To configure a firewall recurring schedule:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Firewall* > *Schedule* > *Recurring* > *Create New*.

Name	Enter the name of the firewall schedule.
Comments	Add comments on the firewall schedule, if any.
Day	Select the days of the week when the schedule applies.
Start	Select the start time for the schedule.
Stop	Select the stop time for the schedule.

4. Select OK.

Configuring firewall schedule groups

You can group the recurring schedules.

Create New	Select to create a firewall recurring schedule group.
Name	The name of the firewall schedule group.
Member	Which recurring schedules are members of the group.
Comments	Comments on the schedule group.
Action	Select the Delete icon to remove a firewall schedule, and Edit icon to modify a firewall schedule.

To create a schedule group:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Firewall* > *Schedule* > *Schedule Group* > *Create New*.

Group Name	Enter the name of the firewall schedule group.
Comments	Add comments on the firewall schedule group, if any.
Available Schedule	List of recurring schedules that are available to be in the schedule group.
Selected Schedule	List of recurring schedules that are members of the group.

4. Select *OK*.

Configuring trusted IPs exempted from intrusion detection

You can specify trusted IP addresses from which traffic will not be scanned for potential intrusion attempts.

To configure trusted IPs:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Firewall* > *Trusted IP* > *Trusted IP Address*.
4. Select *Create New*.
5. Enter a name for the trusted IP address.
6. Do one of the following:
   - From the *Type* list, select *Single Address* and enter the address in the *Single Address* field.
   - From the *Type* list, select *IP Range* and enter the IP address range in the *IP Range* field.
   - From the *Type* list, select *Subnet* and enter the IP address and subnet mask in the *Subnet* field.

7. Select *OK*.
8. In the FortiClient menu, go to *System* > *Trusted IP* > *Trusted IP Setting* and select the *Enable Trusted IP* check box.
9. Select *Apply*.

Configuring ping servers for a FortiClient agent firewall

You can define ping servers that the FortiClient application checks when it is connected to a new network, such as a wireless access point.

Name	Enter the name for the ping server.
Ping Server	The IP address or fully qualified domain name (FQDN) of the server.
Day	Select the days of the week when the schedule applies.
Action	Select Edit to modify the configuration or Delete to remove it.

To configure a firewall ping server:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Firewall* > *Trusted IP* > *Ping Server*.
4. Select *Create New*.
5. Enter a name for the ping server.
6. Enter the IP address or FQDN of the ping server.
7. Select *OK*.

Setting the firewall options of a FortiClient agent

When controlled by FortiManager, the FortiClient application normally blocks all access for which there is no firewall policy and raises a firewall policy violation alert to the FortiManager unit. Optionally, you can change the FortiClient firewall default action to allow all accesses for which there is no Deny firewall policy.

The FortiClient application has three pre-configured firewall profiles: Basic home use, Basic business and Custom. The custom profile is the default. You define firewall policies as needed to allow or deny traffic.

Select a FortiClient agent in the All Managed Clients or Ungrouped Clients lists and select *Firewall* > *Option* to configure the firewall default action.

Override	Select to override the policy inherited from the group to which the computer belongs.
Basic Setting	
Enable Firewall	Select to enable the firewall.

Firewall Profile	Select one of the following profiles. *Basic home use* — Allow all outgoing traffic and deny all incoming traffic. *Basic business* — Allow all outgoing traffic, allow all incoming traffic from the trusted zone, and deny all incoming traffic from the public zone. *Custom profile* — This is the default profile. You can configure firewall policies to control application access to the network and to control traffic between address groups.
When launch new applications	Select firewall action when an unknown application tries to communicate through the firewall: *Ask — The user is asked if the application should be allowed or denied network access. This is the default option.* *Allow* — Allow the application to communicate, but raise a firewall violation alert. *Block* — The application is blocked and raises a firewall violation alert.
Disable task bar notification of blocked network traffic	Do not alert FortiClient user that traffic is blocked.
Enable Trusted IP	Trusted IP addresses, defined in *Firewall* > *Trusted IP* are not scanned for potential intrusion attempts. See “Configuring trusted IPs exempted from intrusion detection” on page 347.
Rules order of global firewall policy	When there are “allow” and “deny” firewall rules in FortiClient, this setting determines the action that has higher priority when rules overlap. **Allow rules first** — When selected, the “allow” firewall rules in FortiClient are processed first. **Deny rule first** — When selected, the “deny” firewall rules in FortiClient are processed first.
Ping Servers	
Use Ping servers to determine the trust status of networks	The FortiClient application checks for response from ping servers you have configured to determine whether it is connected to a trustworthy network. See “Configuring ping servers for a FortiClient agent firewall” on page 348.
Zone Security Setting	Select the security level for the Public and Trusted zones.

Public Zone Security Level	*High* — Block ICMP, NetBIOS, but allow other traffic coming from this zone. *Medium* — Block ICMP and NetBIOS from this zone, but allow other traffic. Allow NetBIOS to this zone. *Low* — Allow all traffic, except where disallowed by application policies. By default, the Public Zone has High security level.
Trusted Zone Security Level	*High* — Block ICMP, NetBIOS, but allow other traffic coming from this zone. *Medium* — Allow all traffic to and from this zone. *Low* — Allow all traffic, except where disallowed by application policies. By default, the Trusted Zone has Medium security level.

Selecting a web filter profile for a FortiClient agent

If Web Filtering is enabled, web filter profiles determine which categories and classifications of URLs are blocked.

To view web filter profiles:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Web Filter* > *Profile*.

Apply to All Members	If you are editing a group profile, select this button to replace web filtering settings on all members with the group settings.
Override	The FortiClient agent's configuration includes settings inherited from the group to which the computer belongs. Selecting override allows you to select a different web filtering profile than the one inherited from the group. Deselecting override means that you want to use the web filtering profile inherited from the group to which the computer belongs. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Web Filter Profile	Select a web filtering profile. For more information, see "Viewing and editing web filter profiles" on page 310. If you select Enable Per User Setting, this profile is applied to users with no assigned web filtering profile.
Enable Per User Setting	For a FortiClient agent that belongs to a Windows AD domain, enable this option to select a web filter depending on the computer user based on information retrieved from Windows AD. See "Working with Windows AD users and groups" on page 315.

Configuring web filter options on a FortiClient agent

You can enable Web Filtering that uses the FortiGuard Web Filtering service to help you control web access by URL. For FortiClient agents and groups, web filtering profiles determine which categories of URLs are blocked and which specific URLs are always blocked or always allowed. See "Viewing and editing web filter profiles" on page 310.

FortiGuard web filtering is a managed Web Filtering solution provided by Fortinet. FortiGuard-Web sorts hundreds of millions of web pages into a wide range of categories users can allow, block, or monitor.

The FortiManager unit can act as the local FortiGuard web filtering service center, overriding the default FortiGuard servers. If you have a large number of FortiClient agents, using this feature speeds up the installation of the web filtering settings.

You can specify a replacement web page for the FortiClient agent to display to users when a URL is blocked because of its category or because it is in the block site list. See "To configure custom web filter block web pages:" on page 352.

To configure web filter options:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Web Filter* > *Option* > *Basic Setting*.
4. Configure the following settings and select *Apply*.

Override	The FortiClient agent's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited FortiGuard server on this FortiClient agent. Deselecting override means that you want to use the FortiGuard server inherited from the group to which the computer belongs. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Enable Web Filter	Select to enable web filtering.
Default behavior for unrated URLs	Select whether to allow or block URLs that are not known to FortiGuard Web. The default is *Allow*.
Log all visited URLs	Log all visited URLs to FortiAnalyzer or syslog server
Disable IP Address Rating	Filter by domain rating only. Sometimes filtering by IP address can produce false positives.
Override Default Web Filter Server	Select to get the web filter settings from the FortiManager unit: • Enter the unit's IP address. • Enter the unit's port number.

To configure custom web filter block web pages:

If the web filter block page is customized, it MUST be written in UTF-8. Because the URL rating category is in UTF-8, the character set cannot be mixed in one page.

Use the following line to help the web browser select the correct code page to display.

```
<meta http-equiv='content-type' content='text/html; charset=UTF-8'>
```

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Web Filter* > *Option* > *Custom Block Page*.
4. Select *Override* to override the group settings for this FortiClient agent.
5. Select *Custom* for the page you want to customize and then do one of the following:
   - Enter the HTML text into the text box.

   or
   - Select *Browse*, find the HTML file of the custom page content and select *Upload*.
6. Optionally, select *Preview* to view the custom page.
7. Select *Apply*.

Configuring Email Filter settings on a FortiClient agent

The email filtering feature filters spam email into a special folder in the Microsoft Outlook or Outlook Express email client on the user's computer. FortiClient first checks email messages against the local black/white list and banned words list. Messages not caught in these filters are filtered using the FortiGuard Email Filter service.

In both the black/white list and banned word filter, you can use a regular expression to create an entry that matches multiple cases.

The FortiManager unit can act as the local FortiGuard Email Filter service center, overriding the default FortiGuard servers. If you have a large number of FortiClient agents, using this feature speeds up the installation of the email filtering settings.

To configure the Email Filter Black/White List:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Email Filter* > *Black/White List*.
4. Do any of the following:
   - To remove an existing entry, select its *Delete* icon.
   - To edit an existing entry, select its *Edit* icon.
   - To add an entry, select *Create New*, select *Block* (black list) or *Allow* (white list), enter the email address and select *OK*.
   - To copy an entry to the client group Black/White list, select its *Copy to group* icon.

To configure the banned word filter:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.

2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Email Filter* > *Banned Word Filter*.
4. Do any of the following:
   - To remove an existing entry, select its *Delete* icon.
   - To edit an existing entry, select its *Edit* icon.
   - To add an entry, select *Create New*, enter the banned word and select *OK*.
   - To copy an entry to the client group banned word filter, select its *Copy to group* icon.

Configuring Email Filter options

You can enable Email Filter, submit mis-rated spam, and set the default Email Filter server.

To set Email Filter options:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient agent you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *Email Filter* > *Option*.
4. Configure the following settings and then select *Apply*.

Override	The FortiClient agent's configuration includes those inherited from the group to which the computer belongs. Selecting override allows you to modify the inherited Email Filter configuration on this FortiClient agent. Deselecting override means that you want to use the configuration inherited from the group to which the computer belongs. See "Adding a FortiClient agent group" on page 302 and "Configuring settings for client groups" on page 304.
Enable Email Filter	Enable the Email Filter feature.
Submit mis-rated Email automatically	Enable this option if you want FortiClient to automatically send mis-rated email to the Fortinet FortiGuard Email Filter service to enhance the service's email-scanning accuracy. A user indicates an email message is mis-rated by selecting Mark Not Spam.
Don't prompt user to submit mis-rated Email	Enable this option if you do not want FortiClient to prompt users to submit mis-rated email messages to the Fortinet FortiGuard Email Filter service. A user indicates that an email message is mis-rated by selecting Mark Not Spam. Users are also not prompted if Submit mis-rated Email automatically is enabled.
Override Default Email Filter Server	Select to get the Email Filter settings from the FortiManager unit: • Enter the unit's IP address. • Enter the unit's port number.

Configuring anti-leak options on a FortiClient agent

Antileak prevents accidental leakage of sensitive information through email messages. When a user on a FortiClient computer sends an email message using Microsoft Outlook, FortiClient searches the attachments for the words or patterns in the antileak sensitive words list. If any of the words or patterns are found, FortiMail logs the message and can also block sending of the message.

To configure the sensitive word list:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *AntiLeak* > *Sensitive Word*.
4. Do any of the following:
   - To remove an existing entry, select its *Delete* icon.
   - To edit an existing entry, select its *Edit* icon.
   - To add an entry, select *Create New*, enter the sensitive word and select *OK*.
   - To copy an entry to the client group sensitive word list, select its *Copy to group* icon.

To configure antileak options:

1. In the *FortiClient Manager*, select *Client/Group* > *Client* > *Managed Client* in the navigation pane.
2. In the *All Managed Clients* list, select the FortiClient computer you want to configure from the *Host Name* column.
3. From the FortiClient menu, select *AntiLeak* > *Option*.
4. Select *Enable AntiLeak*.
5. Select one of the following options:

Log this event	Log outgoing email messages that leak sensitive information.
Block leakage	Block sending of email messages that leak sensitive information. Blocked messages are logged.

6. Select *Apply*.

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
- Monitoring HA status
- Configuring HA options
- 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, FortiGate, FortiMail and FortiClient configuration and related information in the FortiManager database on the FortiManager unit hard disk. The *Device Manager* also stores and manages FortiGate firmware images and optionally FortiGuard service data on the FortiManager unit hard disk.

A key way to enhance reliability of FortiManager is to protect the data in the FortiManager database from being lost if the FortiManager unit fails. This can be achieved by dynamically backing up FortiManager database changes to one or more backup FortiManager units. Then if the operating FortiManager unit fails, a backup FortiManager unit can take the place of the failed unit.

A FortiManager HA cluster consists of up five FortiManager units of the same model. One of the FortiManager units in the cluster operates as a primary or master unit and the other one to four units operate as backup units. All of the units are visible on the network. The primary unit and the backup units can be at the same location. FortiManager HA also supports geographic redundancy so the primary unit and backup units can be in different locations attached to different networks as long as communication is possible between them (for example over the Internet, over a WAN, or through a private network).

Administrators connect to the primary unit Web-based Manager or CLI to perform FortiManager operations. The primary unit also interacts with managed FortiGate, FortiCarrier and FortiMail devices, and FortiClient applications. Managed devices connect with the primary unit for configuration backup and restore. If FortiManager is used to distribute firmware updates and FortiGuard updates to managed devices, the managed devices can connect to the primary unit or one of the backup units.

If the primary FortiManager unit fails you must manually configure one of the backup units to become the primary unit. The new primary unit will have the same IP addresses as it did when it was the backup unit.

When changing a secondary unit in an HA cluster to a primary unit, the FortiManager unit must be rebooted.

Synchronizing the FortiManager configuration and HA heartbeat

All changes to the FortiManager database are saved on the primary unit, and then these changes are synchronized to the backup units. The FortiManager configuration of the primary unit is also synchronized to the backup units (except for the HA parameters). Also, all firmware images and all FortiGuard data stored by the *Device Manager* are synchronized to the backup units. As a result, the backup units always match the primary unit. So if the primary unit fails, a backup unit can be configured to take the place of the primary unit and continue functioning as a standalone FortiManager unit.

While the FortiManager cluster is operating, all backup units in the cluster exchange HA heartbeat packets with the primary unit so that the primary unit can verify the status of the backup units and the backup units can verify the status of the primary unit. The HA heartbeat packets use TCP port 5199. HA heartbeat monitoring, as well as FortiManager database and configuration synchronization takes place using the connections between the FortiManager units in the cluster. As part of configuring the primary unit you add peer IPs and peer serial numbers of each of the backup FortiManager units in the cluster. You also add the peer IP of the primary unit and the primary unit serial number to each of the backup units.

Depending on the peer IPs that you use you can isolate HA traffic to specific FortiManager interfaces and connect those interfaces together so that they function as synchronization interfaces between the FortiManager units in the cluster. Communication between the units in the cluster must be maintained for the HA cluster to operate.

The interfaces used for HA heartbeat and synchronization communication can be connected to your network. However, if possible you should isolate HA heartbeat and synchronization packets from your network to save bandwidth.

If the primary unit or a backup unit fails

If the primary unit fails the backup units stop receiving HA heartbeat packets from the primary unit. If one of the backup units fails, the primary unit stops received HA heartbeat packets from the backup unit. In either case the cluster is considered down until it is reconfigured.

When the cluster goes down the cluster units still operating send SNMP traps and write log messages to alert the system administrator that a failure has occurred. You can also see the failure from the real time monitor and the HA Status page.

You re-configure the cluster by removing the failed unit from the cluster configuration. If the primary unit has failed, this means configuring one of the backup units to be the primary unit and adding peer IPs for all of the remaining backup units to the new primary unit configuration.

When changing a secondary unit in an HA cluster to a primary unit, the FortiManager unit must be rebooted.

If a backup unit has failed, you re-configure the cluster by removing the peer IP of the failed backup unit from the primary unit configuration.

Once the cluster is re-configured it will continue to operate as before but with fewer cluster units. If the failed unit is restored you can re-configure the cluster again to add the failed unit back into the cluster. In the same way you can add a new unit to the cluster by changing the cluster configuration to add it.

FortiManager HA cluster startup steps

FortiManager units configured for HA start up begin sending HA heartbeat packets to their configured peer IP addresses and also begin listening for HA heartbeat packets from their configured peer IP addresses.

When the FortiManager units receive HA heartbeat packets with a matching HA cluster ID and password from another from a peer IP address the FortiManager unit assumes the peer is functioning.

When the primary unit is receiving HA heartbeat packets from all of the configured peers or backup units, the primary unit sets the cluster status to up. Once the cluster is up the primary unit then synchronizes its configuration to the backup unit. This synchronization process can take a few minutes depending on the size of the FortiManager database. During this time database and configuration changes made to the primary unit are not synchronized to the backup units. Once synchronization is complete, if changes were made during synchronization, they are re-synchronized to the backup units.

Most of the primary unit configuration, as well as the entire FortiManager database, are synchronized to the backup unit. Interface settings and HA settings are not synchronized. These settings must be configured on each cluster unit.

Once the synchronization is complete, the FortiManager HA cluster begins normal operation.

Configuring HA options

To configure HA options go to *System Settings* > *General* > *HA*. From here you can configure FortiManager units to start an HA cluster or you can change the HA configuration of the cluster.

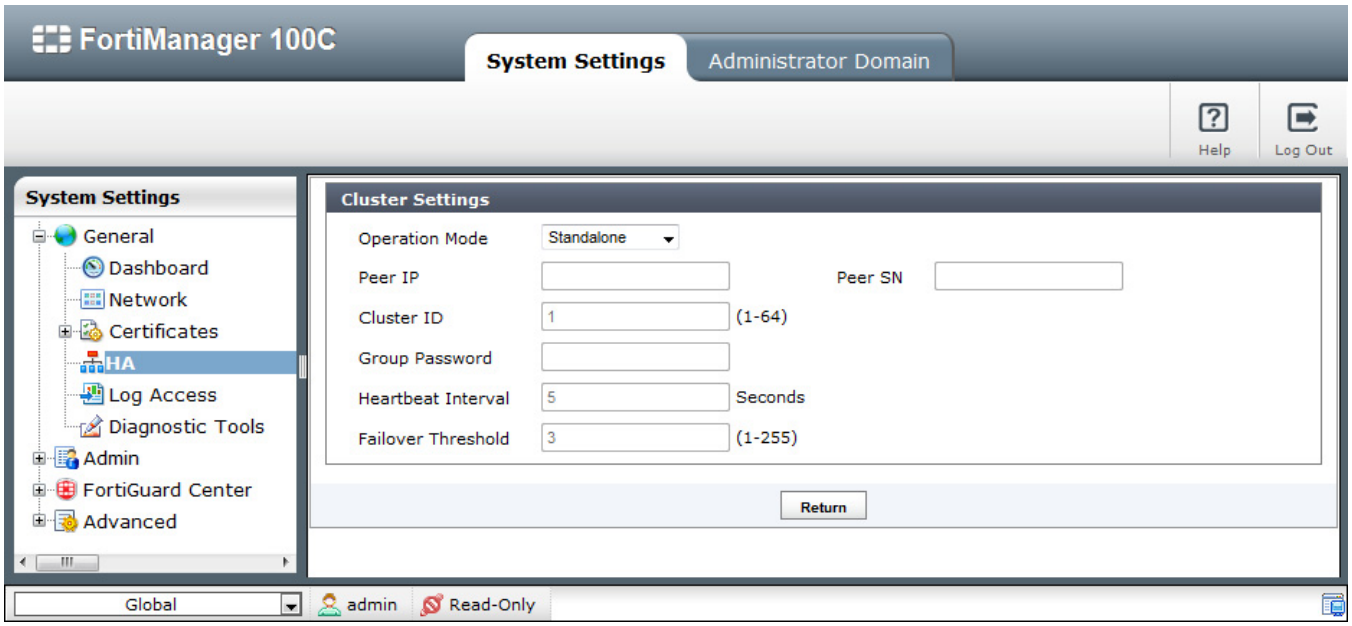
To configure a cluster, you must set the mode of the primary unit to Master and the modes of the backup units to Slave.

When changing the HA mode for a FortiManager unit in an HA cluster, the FortiManager unit must be rebooted.

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

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

Figure 183: Cluster Settings



Cluster Status	Monitor FortiManager HA status. See “Monitoring HA status” on page 363.
Operation Mode	Select *Master* to configure the FortiManager unit to be the primary unit in a cluster. Select *Slave* to configure the FortiManager unit to be a backup unit in a cluster. Select *Standalone* to stop operating in HA mode.
Peer IP	Enter the IP address of another FortiManager unit in the cluster. For the primary unit you can add up to four Peer IPs for up to four backup units. For a backup unit you add the IP address of the primary unit.
Peer SN	Enter the serial number of another FortiManager unit in the cluster. For the primary unit you can add up to four Peer serial numbers for up to four backup units. For a backup unit you add the serial number of the primary unit.
Cluster ID	A number between 0 and 64 that identifies the HA cluster. All members of the HA cluster must have the same group ID. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different group ID. The FortiManager Web-based Manager browser window title changes to include the Group ID when FortiManager unit is operating in HA mode.

Group Password	A password for the HA cluster. All members of the HA cluster must have the same group password. The maximum password length is 19 characters. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different password.
Heartbeat Interval	The time in seconds that a cluster unit waits between sending heartbeat packets. The heartbeat interval is also the amount of time that a FortiManager unit waits before expecting to receive a heartbeat packet from the other cluster unit. The default heartbeat interval is 5 seconds. The heartbeat interval range is 1 to 255 seconds. You cannot configure the heartbeat interval of the backup units.
Failover Threshold	The number of heartbeat intervals that one of the cluster units waits to receive HA heartbeat packets from other cluster units before assuming that the other cluster units have failed. The default failover threshold is 3. The failover threshold range is 1 to 255. You cannot configure the failover threshold of the backup units. In most cases you do not have to change the heartbeat interval or failover threshold. The default settings mean that if the a unit fails, the failure is detected after 3 x 5 or 15 seconds; resulting in a failure detection time of 15 seconds. If the failure detection time is too short the HA cluster may detect a failure when none has occurred. For example, if the primary unit is very busy it may not respond to HA heartbeat packets in time. In this situation, the backup unit may assume that the primary unit has failed when the primary unit is actually just busy. Increase the failure detection time to prevent the backup unit from detecting a failure when none has occurred. If the failure detection time is too long, administrators will be delayed in learning that the cluster has failed. In most cases, a relatively long failure detection time will not have a major effect on operations. But if the failure detection time is too long for your network conditions, then you can reduce the heartbeat interval or failover threshold.

General FortiManager HA configuration steps

The following procedures assume that you are starting with four FortiManager units running the same firmware build and are set to the factory default configuration. The primary unit and the first backup unit are connected to the same network. The second backup units is connected to a remote network and communicates with the primary unit over the Internet.

1. Configure the FortiManager units for HA operation.
   - Configure the primary unit.
   - Configure the backup units.
2. Change the network configuration so that the remote backup unit and the primary unit can communicate with each other.
3. Connect the units to their networks.
4. Add basic configuration settings to the cluster.
   - Add a password for the admin administrative account.
   - Change the IP address and network mask of the port1 interface.
   - Add a default route.

Web-based Manager configuration steps

Use the following procedures to configure the FortiManager units for HA operation from the FortiManager unit Web-based Manager.

To configure the primary unit for HA operation:

1. Connect to the primary unit Web-based Manager.
2. Go to *System Settings* > *General* > *HA*.
3. Configure HA settings.
4. Select Apply.

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.)

5. Power off the primary unit.

To configure the backup unit on the same network for HA operation:

1. Connect to the backup unit Web-based Manager.
2. Go to *System Settings* > *General* > *HA*.
3. Configure HA settings.
4. Select Apply.

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.)

5. Power off the backup unit.

To configure a remote backup unit for HA operation:

1. Connect to the backup unit Web-based Manager.
2. Go to *System Settings* > *General* > *HA*.
3. Configure HA settings.
4. Select Apply.

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.)

5. Power off the backup unit.

To change the network configuration so that the remote backup unit and the primary unit can communicate with each other:

1. Configure the appropriate firewalls or routers to allow HA heartbeat and synchronization traffic to pass between the primary unit and the remote backup unit using the peer IPs added to the primary unit and remote backup unit configurations.

   HA traffic uses TCP port 5199.

To connect the cluster to the networks:

1. Connect the cluster units.

   No special network configuration is required for the cluster.
2. Power on the cluster units.

   The units start and user HA heartbeat packets to find each other, establish the cluster, and synchronize their configurations.

To add basic configuration settings to the cluster:

Configure the cluster to connect to your network as required.

Monitoring HA status

Go to *System Settings* > *General* > *HA* to monitor the status of the FortiManager units in an operating HA cluster. The FortiManager HA status dialog box displays information about the role of each cluster unit, the HA status of the cluster, and also displays the HA configuration of the cluster.

The FortiManager Web-based Manager browser window title changes to indicate that the FortiManager unit is operating in HA mode. The following text is added to the title *HA (Group ID: <group_id>)*. Where <group_id> is the HA Group ID.

From the FortiManager CLI you can use the command `get fmsystem ha` to display the same HA status information.

Figure 184: FortiManager HA status

Cluster Status(Master Mode)

Mode	SN	IP	Enable	Status	Module Data Synchronized (Bytes)	Pending Module Data (Bytes)
Master	FM400B3M08600017	Connecting to Peer				
Slave	42	1.0.0.1	Enabled		0	0
Slave	56	1.0.0.2	Enabled		0	0

Upgrading the FortiManager firmware for an operating cluster

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.

You can upgrade the FortiManager firmware of an operating FortiManager cluster in the same was a upgrading the firmware of a standalone FortiManager unit. During the firmware upgrade procedure, you connect to the primary unit Web-based Manager or CLI to upgrade the firmware. Then install the firmware on the slave units.

Similar to upgrading the firmware of a standalone FortiManager unit, normal FortiManager operations are temporarily interrupted while the cluster firmware upgrades. As a result of this interruption, you should upgrade the firmware during a quiet period.

To upgrade FortiManager HA cluster firmware

1. Log into the primary unit Web-based Manager.
2. Upgrade the primary unit firmware.

   THe firmware is forwarded to all the slave units, and then all the devices (master and slaves) are rebooted.

Administrators may not be able to connect to the FortiManager Web-based Manager until the upgrade synchronization process is complete. During the upgrade, using SSH or telnet to connect to the CLI may also be slow, however use the console to connect to the CLI.

FortiManager Firmware

This section contains instructions to upgrade from the following v4.0 firmware releases to FortiManager v4.0 MR3 Patch Release 8:

- FortiManager v4.0 MR3 Patch Release 1 or later
- FortiManager v4.0 MR2 and Patch Release 1 or later

Firmware upgrades from FortiManager v3.0, v4.0 and v4.0 MR1 are not directly supported. Upgrade the FortiManager to v4.0 MR2 prior to upgrading to v4.0 MR3 Patch Release 8. See *FortiManager v4.0 MR2 Release Notes* for the correct upgrade path.

When upgrading FortiManager VM from v4.0 MR2 to v4.0 MR3 you must apply the appropriate FortiManager VM Base license file and upgrade license file. Contact your Fortinet Partner for more information.

Remember to backup the current FortiManager system before proceeding with the FortiManager v4.0 MR3 Patch Release 8 upgrade.

When upgrading from FortiManager v4.0 MR2 EMS mode, you must run the *Import Wizard* for each managed device to ensure all rules and policies are added to the FortiManager.

Upgrade information

The following table lists the general firmware upgrade steps.

Table 12: General upgrade steps

Step 1	Prepare your FortiManager for the firmware upgrade.
Step 2	Backup your FortiManager database and transfer the v4.0 MR3 Patch Release 8 firmware image.
Step 3	Log into the FortiManager Web-based Manager to verify the upgrade was successful.
Step 4	Populate policies and objects with the import wizard.

Upgrading from FortiManager v4.0 MR3

Step 1: Backup FortiManager database and configuration

Back up the FortiManager v4.0 MR3 database or configuration with the following steps:

1. Login to the FortiManager v4.0 MR3 Web-based Manager.
2. Switch FortiManager to *Standalone* mode if HA is enabled.
3. Go to *System Settings* > *General* > *Dashboard.*
4. Select the *Backup* in the *System Information* widget.
5. Back up all configuration settings.
6. Download the system configuration and database in a .dat file to your local computer.
7. Disable the *Scheduled Backup* feature.

Step 2: Transfer the firmware image to FortiManager

Transfer the new FortiManager v4.0 MR3 Patch Release 8 firmware image to the FortiManager device:

1. Login to the FortiManager v4.0 MR3 Web-based Manager.
2. Go to *System Settings* > *General* > *Dashboard*.
3. Select *Upgrade* in the *System Information* widget.
4. Browse for the FortiManager v4.0 MR3 Patch Release 8 image file.
5. Select *OK*.

After the upgrade, please clear your browser cache before logging into the FortiManager Web-based Manager. Please make sure your computer's screen resolution is set to at least 1280x1024, otherwise, the Web-based Manager may not be displayed properly.

Step 3: Verify the upgrade

After the firmware image has uploaded to the FortiManager and the system successfully rebooted, login to the FortiManager system to verify that the upgrade has completed successfully.

To verify the upgrade:

1. Login to the FortiManager Web-based Manager using the previously configured administrator name and password. Also review all the administrator profiles to configure the proper access privileges.
2. Launch the *Device Manager* tab and make sure that all formerly added FortiOS v4.0 MR2 and v4.0 MR3 devices are still listed.
3. Launch other functional modules and make sure they work properly.

Step 4: Upgrade FortiOS devices

Upgrade all FortiOS v4.0 MR3 devices to v4.0 MR3 Patch Release 12 or later. See *FortiOS v4.0 MR3 Patch Release 12 Release Notes* for the upgrade procedure.

Upgrading from FortiManager v4.0 MR2

Step 1: Prepare FortiManager for upgrade

To prepare your FortiManager for upgrade:

1. Install any pending configurations.
2. Upgrade FortiManager to at least v4.0 MR2. See *FortiManager v4.0 MR2 Release Notes* for the upgrade procedure.
3. Upgrade all managed FortiOS v3.0, v4.0, and v4.0 MR1 devices to v4.0 MR2 or v4.0 MR3 Patch Release 12 or later. See the Release Notes for more information.
4. Disable migration mode on all ADOMs.
5. Switch FortiManager to *Standalone* mode if HA is enabled. FortiManager should finish synchronizing all data between the cluster members.

Step 2: Backup the database and transfer the firmware image

Transfer the new FortiManager v4.0 MR3 Patch Release 8 firmware image to the FortiManager device:

1. Backup FortiManager database. Note that the system backup file from a v4.0 MR2 release cannot be directly imported into a FortiManager v4.0 MR3 system.
2. Transfer the new FortiManager v4.0 MR3 firmware image to your FortiManager.

Step 3: Verify the upgrade

After the firmware image has uploaded to the FortiManager and the system successfully rebooted, login to the FortiManager system to verify that the upgrade has completed successfully.

To verify the upgrade:

1. Login to the FortiManager Web-based Manager using the previously configured administrator name and password. Review all administrator profiles to configure the proper access privileges.
2. Launch the *Device Manager* tab and make sure that all formerly added FortiOS v4.0 MR2 devices are still listed.
3. Perform a *Retrieve* on all v4.0 MR2 devices.
4. Launch other functional modules and make sure they work properly.

Table 13: Supported components

Module/Service	Upgrade Support Status
Device Information and Configuration	Supported
Group Information and Membership	Supported
Revision History	Supported
EMS Global Database	Partially Supported
GMS Security Console	Supported[a]
Real Time Monitor	Not Supported
Scripts	Supported
Service	Supported

Table 13: Supported components (continued)

Firmware	Supported
System Settings	Supported

a. FortiManager may drop all the objects in Security Console if there exists an object with syntax that is not compatible with v4.0 MR2 and MR3. The error will cause a rollback to a default ADOM. If this occurs, please follow Step 4, *Populate Objects and Policy with Import Wizard* to regenerate the ADOM database.

System settings

Please review all administrator profiles to configure the proper access privileges.

EMS global database

Global Database has been replaced by the *Policy & Objects* module. An upgrade does not retain header and footer policies, but it does save the global objects. See Step 4: Populate policy and objects with the import wizard below on how to import objects and policies from a managed device/VDOM to recover the policies.

GMS security console

For VPN console, FortiManager retains all VPNs, but users have to manually redefine all firewall policies related to the VPNs.

To create VPN firewall policies:

1. In the root ADOM, select the *Policy & Objects* module.
2. Under Policy, right-click on the *Local Domain Policies* section and select *Create New* > *Policy.*
3. Define the *Source Zone*, *Source Address*, *Destination Zone*, *Destination Address*, *Schedule*, *Service* and *Action* for the policy and select *OK*.

Figure 185: Right click to create

Step 4: Populate policy and objects with the import wizard

1. Define all global zones in the *Policy & Objects* module if required. Otherwise, proceed to step 2 below.
2. In the *Device Manager* summary page, right-click on the targeted FortiGate device and launch the import wizard.
3. Define all global zone mappings.
4. Import all policies or specify policies to the default or a selected policy package.

Figure 186: Right-click target device and select *Import Config*

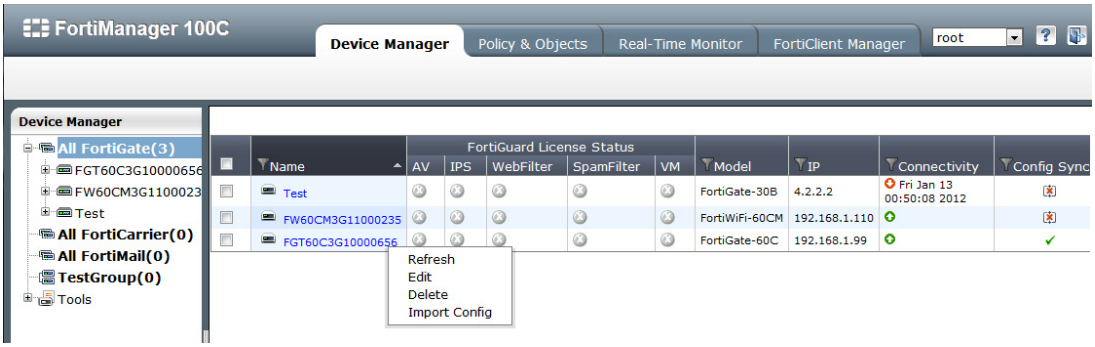
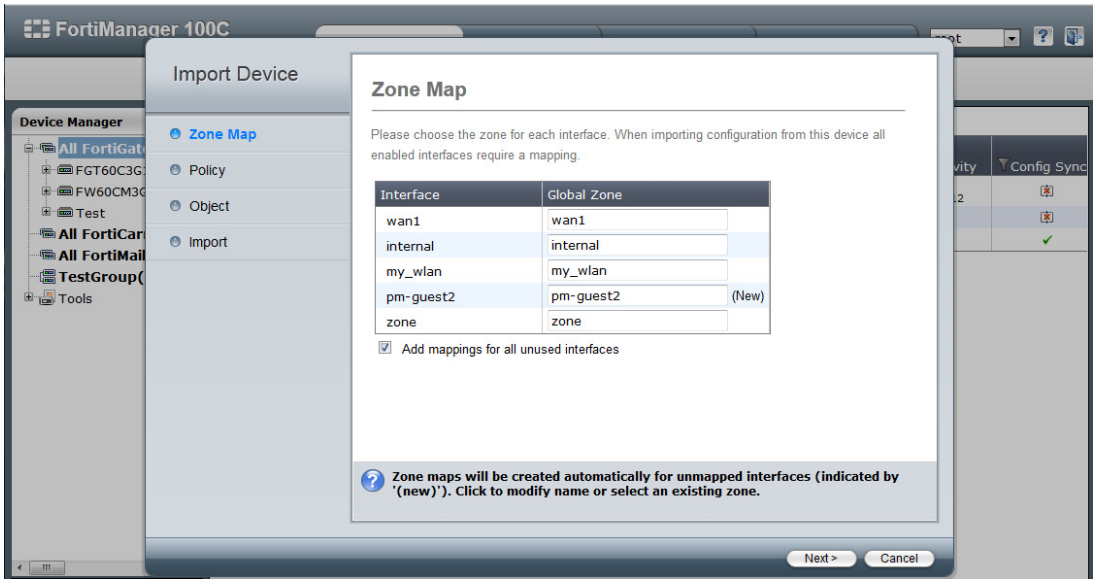


Figure 187: Import Wizard



Header and footer policy upgrade workaround: (optional)

1. Before upgrading to v4.0 MR3, back up the global database objects.
2. In the FortiManager CLI console, run the command `execute fmpolicy printglobal-database <adom name>`, where `<adom name>` is the target ADOM.
3. Copy the output syntax into a text file.
4. Inspect the file for any changes, errors or omissions.
5. Complete the upgrade to v4.0 MR3.
6. In the global *Administrator Domain* module, right click *Global Database* and set to v4.0 MR2.

7. To import the v4.0 MR2 global database backup, edit the output text file to remove the `set srcintf` and `set dstintf` attributes from all header and footer policies.
8. In the global ADOM, select the *Global Policy & Objects* module. Go to *Global Objects* > *Advanced* > *CLI Script*, select the *Import* button.
9. Define a script name, select the CLI backup file and select *OK*.
10. Select the *Run Script Now* button to populate the policies and objects.
11. If an error occurs, inspect the script for errors and run the script again.

Downgrading FortiManager

FortiManager v4.0 MR3 does not provide a full downgrade path. For those users who want to downgrade to an older FortiManager firmware release, downgrade the system firmware via a TFTP server with the firmware burning procedure embedded within the FortiManager system boot-up menu. A full format of the system hard drives and system reset are required after the firmware downgrading process.

All configuration will be lost after downgrading the device, and the system hard drives will be formatted.

Appendix A: Maximum Values/Features

The following table provides a detail summary of maximum values and features on FortiManager platforms.

Table 14: FortiManager maximum values and features

Platform	Devices (Maximum)	ADOMs	Groups	Web Portals	Web Portal Users	Global Policy	Web Portal SDK
FMG-200D	30	30	30	-	-	Yes	-
FMG-400C	300	300	300	-	-	Yes	-
FMG-1000C	800	800	800	800	800	Yes	Yes
FMG-3000C	5000	5000	5000	5000	5000	Yes	Yes
FMG-5001A	4000	4000	4000	4000	4000	Yes	Yes
FMG-VM-Base	10	10	10	10	10	Yes	Yes
FMG-VM-10	+10	+10	+10	+10	+10	Yes	Yes
FMG-VM-100	+100	+100	+100	+100	+100	Yes	Yes
FMG-VM-1000	+1000	+1000	+1000	+1000	+1000	Yes	Yes
FMG-VM-5000	+5000	+5000	+5000	+5000	+5000	Yes	Yes
FMG-VM-U	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Yes	Yes

Appendix B: FortiManager VM

FortiManager VM system requirements

The following table provides a detailed summary on FortiManager VM system requirements.

Table 15: FortiManager VM system requirements

Virtual Machine	Requirement
Hypervisor Support (v4.0 MR3)	VMware ESX version 4.0 and 4.1 Vmware ESXi versions 4.0, 4.1, and 5.0
Virtual Machine Form Factor	Open Virtualization Format (OVF)
Maximum Virtual CPUs Supported (Minimum / Maximum)	1 / Unlimited
Virtual NICs Required (Minimum / Maximum)	1 / 4
Virtual Machine Storage Required (Minimum / Maximum)	80GB / 2TB
Virtual Machine Memory Required (Minimum / Maximum)	1GB / 4GB for 32-bit 1GB / unlimited for 64-bit
High Availability Support	Yes

FortiManager VM licence enhancements

With FortiManager v4.0 MR3 the following changes have been made to FortiManager VM:

- Automatic fifteen (15) day evaluation license
- Removal of requirement to have FortiManager VM contact FortiGuard Distribution Servers (FDS) for license activation
- Stackable license model for FortiManager VM license add-ons
- License can be applied through the FortiManager VM CLI.

Index

A

Active Directory (AD) 315
add content 200
add device 118, 123
add model device 118
address group
  create new 194, 195, 196, 197
administration
  changing access 36
  session timeout 79
Administrative Domains (ADOM)
  administrators 45
administrator
  configure administrator accounts 79
  create a new administrator account 80
  disconnect an administrator 79
  list of administrators 213
  modify an existing administrator account 81
  monitoring administrator sessions 78
  monitoring sessions 78
  trusted host 83
administrator account
  netmask 81, 82
ADOM
  add an ADOM 43
  ADOM device modes 44
  assign an administrator to an ADOM 45
  assign devices to an ADOM 44
  backup mode ADOMs 40
  Concurrent ADOM Access 42
  delete an ADOM 44
  disable the ADOM feature 39
  enable the ADOM feature 39
  normal mode ADOM 40
  view ADOM properties 46
alert console 113
antileak
  options for FortiClient PC 355
antispam
  options 354
  options for FortiClient PC 353
antivirus
  scans 332
  settings 331

B

backing up
  scheduling back ups 66
battery
  pause scanning on battery power 336
browser 32

C

certificates
  creating a local certificate 74
  download a certificate 75
  importing certificates 74
  managing certificates 74
  view certificate details 74
chassis
  add a chassis 158
  dashboard 160
  edit a chassis 159
  enable chassis management 157
  fan tray 160
  managing FortiGate chassis devices 157
  PEM 160, 161
  SAP 160
  shelf manager 160
classification
  web filter 309
CLI
  more 224
  using the console 163
clock 62
cluster, FortiClient Manager
  configuring 311
command line interface (CLI) 49, 59
  Console widget 59
  prompt 61
command prompt 61
configuration
  managing revisions 187
configuration changes, FortiClient
  deploying 306
configuration file, FortiGate
  downloading to a computer 189
  importing from computer 189
configuration, FortiGate
  reverting to another revision 190
configurations, FortiGate
  comparing 189
configuring
  FortiGate unit 150
  VDOMs 151
connecting
  to FDS 252
  to the FortiGuard Distribution Network 248
console 224
Console Access 83
core signature database 337
creating
  VDOMs 152
  web portal user 203

D

dashboard
  add a widget 50
  customizing the dashboard 50
  move a widget 50
  system information 52
  system resource information 53
  view alert messages 58
  view license information 55
  view RAID status 56
  view unit operation 55
  viewing the device summary 55
  widget options 50
deploy licenses
  Free Edition 300
device
  adding 141
  configuring a 150
  deleting 143
  editing FortiGate configuration 143, 156
  importing policies to 145
  refreshing 144
  replacing a FortiGate device 142
  viewing 135
device log 114
discover 118
DNS
  configuring 74
dynamic IP pool
  IP pool 88, 90, 91

E

enabling
  VDOMs 152
  VPN console connections 178
Enterprise license, see also Redistributable
enterprise licensing, FortiClient
  configuring 319
  creating client licenses 320
  creating customized installer 320
event log
  viewing 97
extended signature database 337

F

failover threshold
  HA option 77, 360
failure detection time
  HA 77, 360
fan tray 160
Firewall
  reordering policies 151
firewall address group
  group name 342
firewall address groups
  configuring 342
firewall addresses
  configuring 341
firewall monitor
  viewing 338
firewall policies
  configuring 340
firewall schedules
  configuring 346
firewall services
  configuring 343, 344, 345
firewall, FortiClient
  default action 348
firmware
  changing the firmware on an operating cluster 363
Firmware Manager
  managing FortiGate firmware images 269
  upgrading/downgrading a device/group 269
  upgrading/downgrading FortiManager unit firmware 269
  viewing device firmware images 264
format
  adom file 147
  device format 146
  group file 147
  metadata file 148
  text file 145
FortiClient
  Lockdown 328
FortiClient (FCT)
  discovery 311
  licensing types 319
  lockdown 311
  lockdown settings 311
FortiClient Manager cluster
  configuring 311
FortiClient PC groups
  adding 302
  configuring 304
  deleting 303
  editing 304
  list 302
FortiClient PCs
  All Managed clients list 295
  configuring singly 321
  deleting 300
  resynchronizing 306
  searching 297
  Ungrouped clients list 295
FortiGate
  configuring 150
FortiGate device
  deleting 143
FortiGuard
  AntiVirus and IPS Settings 246
  built-in FDS 249
  FortiGuard Center 243
  Web Filter and Email Filter Settings 247
FortiGuard Services 94
  Configuring 95
  updates 96
Fortinet
  Technical Support 63
Fortinet MIB fields 104
Free Edition 300

G

global
admin settings 93
global objects
searching 192
Global Policies and Objects 191
global resources
VDOMs 154
group ID
HA option 359
group password
HA option 77, 360

H

HA
changing FortiManager firmware 363
configuring HA options 76
configuring High Availability 76
failure detection time 77, 360
monitoring HA status 363
HA options
failover threshold 77, 360
group ID 359
group password 77, 360
heartbeat interval 77, 360
operation mode 77, 359
hard disk 68
heartbeat interval
HA option 77, 360
help 34
host name 61
hot swap 68

I

idle timeout
changing for the web-based manager 36
import
device 117
policies 145

J

Java-based manager
Drag and drop 210
installing 207
logging in 207
Tabs 211
JavaScript 59

L

language 35
changing the web-based manager language 35
web-based manager 35
LDAP
server authentication 89
LDAP servers
for web filtering on Windows network 313
local console access 59
Lockdown
FortiClient 328
log/alert settings
configuring 327
logging
FortiGuard-Web Filter/Antispam events 261
updates and FortiGuard-Web Filter/Antispam 260
updates and FortiGuard-Web Filter/Antispam server 260
updates of managed devices 260
logs 61

M

Main Menu Bar 287
managing
FortiGate firmware images 269
port conflicts for FortiGate devices 249
manually updating antivirus and attack definitions 254
metadata
adding 106, 107
configure 105
FortiGate object 107
requirements 105
MIB 104
FortiGate 102
RFC 1213 102
RFC 2665 102
monitoring
administrator sessions 78
HA status 363
more (CLI command) 224

N

NAT traversal 250
netmask
administrator account 81, 82
network interface
configuring 72
Network Time Protocol (NTP) 61

O

offline mode 109
online help 34
operation mode
HA option 77, 359
option
FortiClient firewall default action 348
override server 248, 252

P

pending actions
managing 326
policies
reordering on first installation 151
pop-up windows 271
port
number 35
port forwarding 250
portal properties 202
power entry modeules (PEM) 161
power entry module (PEM) 160

Premium license, see also Volume license
primary
FortiClient Manager cluster role 312
profile
web portal, configuring 199
prompt 59

R

RADIUS
server authentication 87
server configuration 88
RADIUS server
configuring 88, 89, 91, 92
server secret 88, 90, 92
RAID levels
RAID 0 68
RAID 10 68
RAID 5 68
RAID1 68
Real-Time Monitor (RTM) 270
reboot the FortiManager unit 37
resolution 32
resource limit
VDOMs 154
RFC 1213 102
RFC 1215 103
RFC 2665 102
routing table 72
configuring 72
RTM 270
RTM dashboard 271

S

scans
antivirus 332
scheduling 61
script
cloning 219
creating or editing 218
exporting 220
scheduling 215
Tcl scripts 225
troubleshooting tips 224
secondary
FortiClient Manager cluster role 312
Secure Shell (SSH) 59
security policy
for FortiClient PCs, setting 329
serial number 52, 142
shelf alarm panel (SAP) 160, 163
shelf manager 160
shutdown the FortiManager unit 37
simple network management protocol (SNMP)
system name 61
SNMP 98
community 100
community, configuring 100
configure 99
MIBs 102
RFC 12123 102
RFC 1215 103
RFC 2665 102
traps 103
SNMP manager 104
SNMP, MIB 104
special characters 61
SSL 61
static route
configuring 72
String transliterations 148
sync interval 62
syslog server 112
system settings
FortiClient Manager, configuring 310

T

TACACS+
server authentication 91
Telnet 59
temporary clients
working with 298
time 61
traps
SNMP 103
trusted FortiManager unit
adding a 325
trusted host
security issues 83

U

unlicensed clients list 299
updates
connecting to the FDN 248
connecting to the FDS 252
logging FortiGuard-Web Filter/Antispam events 261
logging updates and FortiGuard-Web Filter/Antispam server 260
logging updates of managed devices 260
managing port conflicts 249
updating antivirus and attack definitions manually 254
updating antivirus and attack definitions manually 254
upgrading firmware
on an HA cluster 363
upgrading/downgrading FortiManager firmware 269
uptime 53
US-ASCII 61
using web portal 204

V

VDOMs
- configuring 151
- creating 152
- enabling 152
- global resources 154
- resource limit 154

viewing firmware images, devices 264
virus
- detected, FortiClient PCs 331

Volume license 308
VPN
- configuring 178
- create a firewall address 178
- create a VPN configuration 178
- create VPN firewall policies 185
- enabling 178
- gateway 183
- settings 328

W

web browser 32
web filter
- classification 309
- configuring LDAP servers 313
- configuring profiles 351
- enabling and options 352

web portal
- add a logo 202
- add content 200
- configuring 198
- configuring profile 199
- creating user 203
- portal properties 202
- using 204

Web Portal Service Development Kit 206
web proxy 248, 251
Web Services
- enabling 205

Web Services Description Language 109
web-based manager
- changing the language 35
- idle timeout 36
- language 35

window
- FortiClient Manager 286

wizards
- add device 116, 123
- device import summary 122
- device settings 131
- global zone map 125
- import device 117
- importing into FortiManager 122
- install 127
- launching the Add Device wizard 116
- policy validation 129
- zone validation 129

WSDL file 109, 206
- obtaining 206

X

XML API 205