FortiManager v5.0 Patch Release 5
Administration Guide



FortiManager v5.0 Patch Release 5 Administration Guide

May 13, 2014

02-505-184107-20140513

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet Document Library	docs.fortinet.com
Fortinet Video Library	video.fortinet.com
Fortinet 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 **12**
Change Log **19**
Introduction **20**
About this document 20
FortiManager documentation 21
What's New in FortiManager v5.0 ..... **22**
FortiManager v5.0 Patch Release 5 22
Policy package scheduled install 22
Install summary page 22
Routing query in DVM table 22
VPN Console supports NAT device with a public IP feature 22
Enable/disable the FortiAnalyzer feature set 23
Manage FortiAnalyzer devices using the FG-FM protocol 23
View license status of managed devices 23
Summary of enhancements 24
FortiManager v5.0 Patch Release 4 24
ADOM firmware version support 24
System dashboard widgets 24
Templates 24
Report templates 25
Summary of enhancements 25
FortiManager v5.0 Patch Release 3 26
RAID Management page 26
FortiMail/FortiWeb logging and reporting support 26
ADOM for FortiCarrier 27
Drill Down tab 27
Event Management tab 27
FortiManager VM support for Microsoft Hyper-V Server 27
Import and export report templates 27
RTM profiles 27
Vertical view 27
Summary of enhancements 27
FortiManager v5.0 Patch Release 2 28
Log arrays 28
Summary of enhancements 29
FortiManager v5.0 Patch Release 1 29
Summary of enhancements 29
FortiManager v5.0.0 29
Device manager layout 30

ADOM properties 30
Device dashboard 30
Policy package status 30
Device profiles 31
Extend workspace to entire ADOM 31
Quick install 32
Bind zone to an address 32
Policy & Objects dual pane 32
Policy package granularity 32
Reports tab 33
Endpoint management 33
Advanced features improvements 34
High Availability takeover without reboot 34
IPv6 administration 34
Single interface zones 35
Summary of enhancements 35
Fortinet Management Theory 37
Key features of the FortiManager system 37
Configuration revision control and tracking 37
Centralized management 37
Administrative domains 37
Local FortiGuard service provisioning 37
Firmware management 37
Scripting 38
Logging and reporting 38
Fortinet device life cycle management 38
Inside the FortiManager system 38
Inside the FortiManager device manager tab 39
Using the Web-based Manager 40
System requirements 40
Supported web browsers 40
Monitor settings for Web-based Manager access 40
Connecting to the Web-based Manager 41
Web-based Manager overview 42
Viewing the Web-based Manager 42
Using the navigation pane 43
Configuring Web-based Manager settings 44
Changing the Web-based Manager language 44
Administrative access 45
Restricting Web-based Manager access by trusted host 46
Changing the Web-based Manager idle timeout 46
Other security considerations 46

Reboot and shutdown of the FortiManager unit 47
Administrative Domains 48
Enabling and disabling the ADOM feature 49
ADOM modes 50
Switching between ADOMs 50
Normal mode ADOMs 50
Backup mode ADOMs 50
ADOM versions 51
Managing ADOMs 51
Extend workspace to entire ADOM 51
Concurrent ADOM access 52
Adding an ADOM 52
Deleting an ADOM 54
Upgrading an ADOM 54
Assigning devices to an ADOM 55
Assigning administrators to an ADOM 56
Locking an ADOM 56
System Settings 57
Dashboard 59
Customizing the dashboard 60
System Information widget 62
System Resource widget 70
License Information widget 72
Unit Operation widget 74
Alert Messages Console widget 74
CLI Console widget 75
Log Receive Monitor widget 76
Logs/Data Received widget 78
Statistics widget 79
All ADOMs 79
RAID Management 80
Network 85
Viewing the network interface list 86
Configuring network interfaces 87
Configuring static routes 88
Configuring IPv6 static routes 89
Diagnostic tools 90
High Availability 90
Configuring HA options 90
Admin 92
Monitoring administrator sessions 92
Administrator 94
Profile 98
Remote authentication server 101

Administrator settings 105
Certificates 107
Creating a local certificate 108
Importing certificates 109
Importing CRLs 109
Viewing certificate details 109
Downloading a certificate 111
Event Log 111
Task Monitor 113
Advanced 114
SNMP v1/v2c 115
Mail Server 121
Syslog Server 122
Meta Fields 123
Device Log Settings 125
Advanced Settings 127
Device Manager 129
Device Manager tab 129
Device Manager tab layout 129
Device policy package status 130
Device profiles 131
Wireless profiles 131
Extend workspace to entire ADOM 131
Quick install 132
Viewing managed device 132
Using column filters 132
View managed devices 133
Dashboard widgets 142
Zone & Interface 145
Log Setting 146
Unregistered devices 146
Administrative domains (ADOMs) 147
Managing devices 147
Adding a device 147
Replacing a managed device 148
Editing device information 150
Refreshing a device 152
Install policy package and device settings 152
Importing and exporting device lists 152
Setting unregistered device options 158
Configuring devices 159
Configuring a device 159
Configuring virtual domains (VDOMs) 160

Log arrays 165
Access points 166
FortiAP clients 168
Rogue APs 169
Working with device groups 170
Managing FortiGate chassis devices 171
Viewing chassis dashboard 173
Using the CLI console for managed devices 177
Provisioning Templates 177
System Templates 177
WiFi Templates 179
Endpoint Templates 195
Certificate Templates 203
FortiManager Wizards 206
Add device wizard 206
Launching the add device wizard 207
Add device wizard options 207
Add a device using the add device wizard (Discovery mode) 209
Add a device using the add device wizard (Add model device) 219
Install wizard 224
Launching the install wizard 224
Install policy package and device settings 224
Installing device settings 228
Import policy wizard 231
Quick install 235
Device Configurations 236
Checking device configuration status 236
Managing configuration revision history 238
Downloading and importing a configuration file 240
Comparing different configuration files 240
Advanced Features 242
Scripting 242
Configuring scripts 243
Script history 248
Script samples 249
CLI scripts 250
CLI script samples 250
TCL scripts 256
Configuring web portals 271
Creating a web portal 272
Configuring the web portal profile 273
Creating a portal user account 276
External users 276

Using the web portal ... 277
Policy & Objects ... 278
About policies ... 279
Policy theory ... 279
Global policy packages ... 281
Policy workflow ... 281
Provisioning new devices ... 281
Day-to-day management of devices ... 282
Display Options ... 282
Managing policy packages ... 283
Lock an ADOM ... 284
Create a new policy package or folder ... 284
Remove a policy package or folder ... 286
Rename a policy package or folder ... 286
Assign a global policy package ... 286
Install a policy package ... 287
Re-install a policy package ... 287
Schedule a policy package install ... 287
Export a policy package ... 288
Edit the installation targets for a policy package ... 288
Perform a policy consistency check ... 289
Managing policies ... 291
Lock an ADOM ... 291
Create a new policy or identity policy ... 291
Interface Policy ... 306
Central NAT table ... 311
IPv6 Policy ... 312
IPv6 Interface Policy ... 312
DoS Policy ... 312
IPv6 DoS Policy ... 318
NAT46 Policy ... 318
NAT64 Policy ... 324
Insert a policy ... 330
Edit a policy ... 330
Clone a policy ... 330
Copy, cut, and paste a policy ... 331
Delete a policy ... 331
Add a section ... 331
Installation page ... 331
ADOM revisions ... 333
VPN Console ... 338
VPN topology ... 338
VPN gateway ... 343
VPN security policies ... 348

Managing objects and dynamic objects 350
Lock an ADOM 354
Create a new object 354
Map a dynamic object 354
Remove an object 356
Edit an object 356
Clone an object 356
Search where an object is used 356
Search objects 357
Drag and drop objects 357
FortiToken configuration example 357
Log View 359
Viewing log messages 360
Customizing the log view 367
Log details 369
Archive 370
Browsing log files 371
Importing a log file 373
Downloading a log file 374
FortiClient logs 375
Configuring rolling and uploading of logs 375
Drill Down 380
Traffic activity 380
Web activity 381
Email activity 381
Threat activity 382
Event Management 383
Events 383
Event details 384
Acknowledge events 385
Event handler 386
Traffic log events 389
Event log alerts 391
Reports 396
Report templates 397
Configure reports 406
Schedules 422
Filters 423
Language & Print options 424
Reports 424
Chart library 426
Chart builder wizard 426
Advanced chart option 430

Report calendar 434
Advanced 434
Dataset 434
Output profile 439
Language 441
FortiGuard Management 443
Advanced settings 444
Connecting the built-in FDS to the FDN 453
Configuring devices to use the built-in FDS 454
Matching port settings 454
Handling connection attempts from unregistered devices 455
Configuring FortiGuard services 455
Enabling push updates 455
Enabling updates through a web proxy 456
Overriding default IP addresses and ports 457
Scheduling updates 458
Accessing public FortiGuard web and email filter servers 458
Logging events related to FortiGuard services 459
Logging FortiGuard antivirus and IPS updates 459
Logging FortiGuard web or email filter events 460
Restoring the URL or antispam database 461
Licensing status 461
Package management 462
Receive status 462
Service status 464
Query server management 465
Receive status 465
Query status 466
Firmware images 468
High Availability 470
HA overview 470
Synchronizing the FortiManager configuration and HA heartbeat 471
If the primary unit or a backup unit fails 471
FortiManager HA cluster startup steps 472
Configuring HA options 472
General FortiManager HA configuration steps 474
Web-based Manager configuration steps 475

Monitoring HA status 477
Upgrading the FortiManager firmware for an operating cluster 478
FortiManager Firmware 479
Upgrading from FortiManager v5.0.0 or later 479
Upgrading from FortiManager v4.0 MR3 479
General firmware upgrade steps 480
Upgrading the FortiManager firmware for an operating cluster 485
Downgrading to previous firmware versions 486
Special notices 486
FortiOS features currently not supported by FortiManager 486
FortiGate firmware upgrade 486
System time on FortiManager VM 486
Memory requirement for FortiManager VM64-HV 486
ADOM for FortiCarrier 487
FortiOS v5.0 override server setting for FortiGuard Services 487
Update services provided to FortiGate v4.0 MR2 or FortiMail devices 488
Log arrays 488
Endpoint management 489
FortiManager VM license check 489
Multi-language display support 489
New hard disk drive partition layout 489
Importing a FortiManager generated policy 489
Importing profile group and RADIUS dynamic start server 489
Push update in bi-directional static NAT 490
Appendix A: FortiManager VM 491
Licensing 491
FortiManager VM firmware 492
Appendix B: Maximum Values 493
FortiManager maximum values 493
Appendix C: License Information API 494
getDeviceLicenseList 494
Index 497

Table of Figures

Management model 39
Web-based Manager 42
Administration settings 45
Management Interface page 45
Enabling ADOMs 49
Create ADOM dialog box 53
Upgrade an ADOM 55
FortiManager system dashboard 59
Adding a widget 60
A minimized widget 61
System Information widget 62
Edit Host Name dialog box 64
Time Settings dialog box 64
Firmware upgrade 66
Backup dialog box 67
Restore dialog box 68
System checkpoint table 69
Create new system checkpoint 69
System checkpoint table 69
System checkpoint table 70
System Resource widget (Real Time display) 70
System Resource widget (Historical display) 70
Edit System Resources Settings window 71
VM License Information widget 72
Change the encryption mode 73
Unit Operation widget 74
Alert Message Console widget 75
List of all alert messages 75
CLI Console widget 76
Log receive monitor widget (log type) 76
Log receive monitor widget (device) 77
Edit log receive monitor settings 77
Logs/data received widget (real-time) 78
Logs/data received widget (historical) 78
Edit logs/data received settings window 78
Statistics widget 79
All ADOMs 79
RAID Management page 81
RAID settings 82
Network screen 85
Network interface list 86
Configure network interfaces 87
Routing table 88
Create new route 88
Create new IPv6 route 89
Diagnostic tools 90
Cluster settings dialog box 90

Administrator session list 93
Administrator list 94
Creating a new administrator account 95
Administrator profile list 98
Create new administrator profile 99
Remote authentication server list 101
New LDAP server dialog box 102
New RADIUS Server window 103
New TACACS+ server dialog box 104
Administrative settings dialog box 105
New local certificate 108
Local certificate detail 110
Event log table 111
Filter settings window 113
Task monitor window 113
SNMP configuration 115
FortiManager SNMP community 117
Mail server window 121
Mail server settings 121
Syslog server window 122
Syslog server settings 122
Metadata 123
Add a meta field 124
Device log setting window 125
Advanced settings 127
WSDL file 128
Device Manager layout 130
Device panel categories 134
Customize tabs 135
Routing query output 141
FortiGate unit dashboard 142
Zone & Interface page 145
Log Setting page 146
View all managed devices from the CLI 149
Edit a device 150
Connection Summary widget 152
Unregistered device dialog box on login 158
Create a new NAT VDOM 161
Create a new transparent VDOM 162
New VDOM link 163
Resource usage page 164
Create log array window 165
Edit FortiAP 167
Upgrade firmware 168
Rogue AP list 169
Adding a group 170
Add a new chassis 172
CLI console 177
System Templates 178
SSIDs list 179
New SSID 180
Import SSID 185

Wireless profiles 186
New AP profile 187
Import wireless profile 190
New WIDS profile 192
Import WIDS profile 194
New endpoint profile 196
FortiClient configuration deployment for Windows and Mac 197
FortiClient configuration deployment for iOS 199
FortiClient configuration deployment for Android 200
Threat level definitions 202
New certificate template 204
Discover mode 207
Add model device mode 208
Discover phase 209
Add device phase 210
Device created successfully 211
Device profile phase 212
Import virtual domains phase 213
Zone map phase 214
Import policy database phase 215
Object phase 216
Download conflict file 216
Objects to import 217
Import phase 217
Summary phase 218
Import report sample 218
Add a VDOM 219
Login phase 220
Add device phase 221
Device created successfully 222
Device profile phase 223
Summary phase 223
Install policy package and device settings 224
Device selection phase 225
Validation phase 226
Policy package installation window 227
Device installation history 227
Install device settings only 228
Device selection window 228
Validation phase 229
Device settings successful installation window 230
Device installation history 230
Zone map phase 231
Policy phase 232
Object phase 233
Import phase 233
Summary phase 234
Summary example 234
Select re-install 235
Configuration and Installation Status widget 236
Revision history tab 238
Add a tag to a configuration version 239

Revision diff dialog box 241
Script list 243
Execute script dialog boxes 244
Create a new script 245
Clone script dialog box 247
Import script dialog box 248
Script execution history table 249
Script history dialog box. 249
Web portal window 272
Add profile dialog box 272
Blank web portal window 273
Adding web portal content 274
Logo preferences 275
Portal properties window 275
Add user dialog box 276
Add external user window 277
Web portal 277
ADOM Level Policy & Objects 278
Management model 279
ADOM level display options 282
Global level display options 283
Create new policy package 285
Installation Targets 285
ADOM assignment list 286
Assign dialog box 286
Scheduled Install 287
Create Install Schedule 288
Edit Install Schedule 288
installation target 289
Consistency Check dialog box 290
Consistency check results window 290
Create new policy 292
Create new policy (VPN) 298
Edit Recurring Schedule 300
Create new identity policy 301
Edit Recurring Schedule 302
Edit Service 303
Profile right-click menu 305
Interface Policy 306
Edit Service 308
Add Install On 310
Central NAT 311
New DoS Policy 313
Edit Service 315
Add Install On 317
NAT46 Policy 319
Edit Recurring Schedule 320
Edit Service 321
Add Install On 324
NAT 64 Policy 325
Edit Recurring Schedule 326
Edit Service 327

Add Install On 330
Editing a policy 330
Installation page 331
ADOM revisions 333
Create new ADOM revision 334
ADOM revision deletion configuration 335
ADOM Revision Diff 336
Details page 337
Restore confirmation 337
Restore Revision 337
Create VPN Topology 338
Add VPN External Gateway (Dial up topology) 343
Add VPN Managed Gateway (Dial up topology) 345
Objects list 350
Create new firewall address object 354
Map Dynamic Address dialog box 355
Dynamic object mappings 355
Where Used dialog box 356
New local user window 358
Traffic log window (Formatted) 360
Traffic log window (Raw) 367
Filter settings dialog box 367
Column settings dialog box 368
Column settings dialog box 368
Filter settings dialog box 369
Log details frame 369
Log archive tab 370
View packet log dialog box 370
Log file list window 371
Display logs by serial number example 373
Import log file dialog box 373
Download log file dialog box 374
FortiClient logs 375
Device log settings window 376
Drill Down tab and data 380
Events page 383
Event details page 385
Confirmation dialog box 385
Event handler page 387
Create event handler page 389
Create event handler page 392
Edit event handler page 394
Default report page 403
Create report page 406
Template page 407
Template and section toolbars 408
Default new report 408
Add a new section 409
Edit section 410
Add a new chart 411
Chart filters dialog box 412
Edit predefined chart 413

Clone chart 413
Choose a graphic dialog box 414
Heading element 414
Edit heading dialog box 415
Edit text dialog box 416
Cover Page Settings page 418
Edit workspace window 419
Move a report template element 420
Edit an element 421
Schedule a report template 422
Report filters 423
Language & Print Options 424
Latest reports 424
Device reports 425
Choose data page 426
Add filters page 427
Preview page 429
Charts page 430
Create new chart (table) dialog box 431
Clone chart dialog box 432
Edit chart dialog box 433
Report calendar 434
Datasets 435
New dataset dialog box 435
Clone dataset dialog box 437
Edit dataset dialog box 437
SQL query pop-up window 438
Output profile page 439
Create new output profile dialog box 440
Report language 441
Create a new language 442
FortiGuard Center advanced settings 445
FortiGuard Center advanced settings (FortiGuard server communication disabled) 448
FortiGuard antivirus and IPS settings 449
FortiGuard web filter and email filter settings 451
Override FortiGuard server 452
Overriding FortiGuard Server 459
Licensing status page 461
FortiGuard package receive status 463
Change deployed package version 464
Update history example (AV Flow Database) 464
Package service status 464
Query receive status 465
Package update history 466
Query status example 467
Firmware images list 468
Firmware images import page 469
Local firmware images 469
Cluster settings 473
FortiManager HA status 477
Firmware images page 480
Example FTP directory 481

Firmware image checksum page 481
Backup dialog box 482
Snapshot of FortiManager VM (VMware) 483
Snapshot of FortiManager VM (Microsoft Hyper-V) 483
Firmware upgrade dialog box 484
Firmware upgrade successful dialog box 484
Verify device connectivity 485

Change Log

Date	Change Description
2012-10-30	Initial release.
2013-04-09	Updated for FortiManager v5.0 Patch Release 2.
2013-04-10	Updated HA firmware instructions.
2013-04-22	Updated available device tabs list.
2013-07-19	Updated for FortiManager v5.0 Patch Release 3.
2013-08-19	ADOM firmware version support information added.
2013-09-13	Updated for FortiManager v5.0 Patch Release 4.
2013-11-18	Updated for FortiManager v5.0 Patch Release 5.
2014-05-13	Removed references to Java Client.

Introduction

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

Using the FortiManager system, you can:

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

FortiManager systems scale to manage up to 10 000 devices and virtual domains (VDOMS) from a single FortiManager interface. FortiManager is designed for medium to large enterprises and managed security service providers. FortiManager system architecture emphasizes reliability, scalability, ease of use, and easy integration with third-party systems.

This section contains the following topics:

- About this document
- FortiManager documentation

About this document

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

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



This is a provisional document.

FortiManager documentation

The following FortiManager product documentation is available:

- *FortiManager v5.0 Patch Release 5 Administration Guide*

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

- *FortiManager device QuickStart Guides*

  These documents are included with your FortiManager system package. Use these document to install and begin working with the FortiManager system and FortiManager Web-based Manager.

- *FortiManager online help*

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

- *FortiManager v5.0 Patch Release 5 CLI Reference*

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

- *FortiManager v5.0 Release Notes*

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

- *FortiManager Log Message Reference*

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

What's New in FortiManager v5.0

FortiManager v5.0 Patch Release 5

FortiManager v5.0 Patch Release 5 includes the following new features and enhancements. Always review all sections in the *FortiManager Release Notes* prior to upgrading your device.



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

Policy package scheduled install

A new item has been added to the right-click menu to create a scheduled Policy Package installation. You can create an install schedule to install the latest changes in the package. When enabled, an icon is displayed beside the package in the Policy Package tree. You can select to edit the schedule or cancel the schedule.

See "Schedule a policy package install" on page 287 for more information.

Install summary page

A new installation status page for policy packages within an ADOM has been added. This page displays the connection status, policy package status, and device settings status.

See "Installation page" on page 331 for more information.

Routing query in DVM table

A routing query has been added to the Device Manager device dashboard tool. You can select a device in the ADOM and select *Menu* > *Query* |> *Routing* to view the routing information for the device. This page displays IP version, type, subtype, network, gateway, interface, up time, distance, and metric.

See "Dashboard toolbar" on page 134 for more information.

VPN Console supports NAT device with a public IP feature

A *public-ip* field has been added to the *Advanced Options* menu when defining a Managed Gateway in VPN console. Use this field to define a public IP address to which the IPsec VPN tunnel needs to be established, when the FortiGate is behind a device performing NAT.

This field can also be used in the following situations:

- A VPN node has the *Local Gateway* field configured, in order to establish the IPsec tunnel to a configured secondary IP, on a FortiGate's default VPN interface. Set the *public-ip* field with the same value as the local gateway, so that the remote VPN peers establish the IPsec tunnel to that secondary IP, instead of the default VPN interface IP.

- The FortiGate's default VPN interface is configured to use a dynamically assigned IP via DHCP or PPPoE, and once attributed, this IP address remains static. VPN Console will normally fail during the install process, stating that the FortiGates's VPN interface does not have an IP or is configured with an IP value of 0. The solution is to configure the dynamically assigned IP value in the *public-ip* field for that FortiGate device.

See "VPN Console" on page 338 for more information.

Enable/disable the FortiAnalyzer feature set

In FortiManager v5.0 Patch Release 5 or later, the FortiAnalyzer feature set (Log View, Drill Down, Event Management, and Reports) is disabled by default. To enable these features, enter the following CLI commands:

```
config system global
  set faz-status enable
end
Changing faz status will affect FAZ feature in FMG. If you continue,
     system will reboot to add/remove FAZ feature.
Do you want to continue? (y/n)
```

Enter `y` to continue, your FortiManager will reboot with the FortiAnalyzer features enabled. If you are not using these features, you can select to disable the FortiAnalyzer feature set.

Manage FortiAnalyzer devices using the FG-FM protocol

You can now add FortiAnalyzer devices to FortiManager as a managed device. You can configure a managed FortiGate device to send logs to one of the managed FortiAnalyzer devices. FortiAnalyzer devices are added to a default FortiAnalyzer ADOM.

See "System Templates" on page 177 for more information.

View license status of managed devices

You can view the license status of devices managed by your FortiManager. The Licensing Status page displays the status of the support contract and modules. You can select to display only devices with expired support contracts.

See "Licensing status" on page 461 for more information.

Summary of enhancements

The following is a list of enhancements in FortiManager v5.0 Patch Release 5:

- Manage FortiAnalyzer devices using the FG-FM protocol
- View license status of managed devices
- FortiController 5103B Dual Mode support
- VPN Console supports NAT device with a public IP feature
- Additional filter for IPS and Application Control profiles
- Routing query in DVM table
- Policy package scheduled install
- ADOM access via TACACS+ attribute
- Where Used search in all ADOMs
- Policy drag & drop extension
- Script management enhancements
- Enable/disable the FortiAnalyzer feature set

FortiManager v5.0 Patch Release 4

FortiManager v5.0 Patch Release 4 includes the following new features and enhancements. Always review all sections in the *FortiManager Release Notes* prior to upgrading your device.



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

ADOM firmware version support

ADOMs can now manage FortiGate devices running different firmware versions.

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

See "ADOM versions" on page 51 for more information.

System dashboard widgets

Three new widgets have been added to the system dashboard: Statistics, Logs/Data Received, and Log Receive Monitor. See "Statistics widget" on page 79, "Logs/Data Received widget" on page 78, and "Log Receive Monitor widget" on page 76 for more information.

Templates

Certificate templates have been moved to *Device Manager* > *Provisioning Templates* > *[ADOM]* > *Certificate Templates*.

Endpoint templates, including endpoint profiles and client reputations have also been added to the template section. See "Provisioning Templates" on page 177.

Report templates

FortiManager v5.0 Patch Release 4 includes the following report templates:

- Admin and System Events Report
- Application and Risk Analysis
- Bandwidth and Applications Report
- Client Reputation
- Email Report
- Security Analysis
- Threat Report
- User Report
- User Security Analysis
- VPN Report
- Web Usage Report
- Wifi Network Summary
- Wireless PCI
- FortiMail Default Report
- FortiWeb Default Report

For more information, see “Reports” on page 396.

Summary of enhancements

The following is a list of enhancements in FortiManager v5.0 Patch Release 4.

FortiManager

- ADOM migration support
- 64-bit version of FortiManager OS for FMG-1000C, FMG-3000C, and FMG-4000D
- Logging support to multiple FortiAnalyzer units
- Policy & object change notification system
- Upgrade v4.0 MR3 based ADOMs to v5.0

  All database objects and Global database will be converted to 5.0 format

Reports

- Option to remove the FortiManager report cover page
- Generate per user reports (setup via XML)
- Chart builder wizard
- Pre-defined report template for custom application report
- Pre-defined report template for threat activity
- Change the background color, text color, text size, and text style in reports
- Format text areas and headers in report
- Report cover page customization
- Usability enhancements for reports

Logging

- SQL index performance optimizations and enhanced log search support
- Import logs from a remote FTP/SCP/SFTP server
- Configure up to three log rolling upload servers

Other

- Export and import image files along with report DAT files
- Event Management extensions and enhancements

FortiManager v5.0 Patch Release 3

FortiManager v5.0 Patch Release 3 includes the following new features and enhancements. Always review all sections in the *FortiManager Release Notes* prior to upgrading your device.



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

RAID Management page

A RAID Management menu item replaces the RAID Monitor widget. This enhancement extends the existing RAID monitoring capabilities allowing you to perform simple RAID management tasks such as add, remove, or replace disks and reconfigure RAID levels.

This page provides a summary of RAID information including the RAID level configured, status, disk space usage, and disk status. When hovering your mouse cursor over each disk, a pop-up window provides the disk number, model, firmware, RAID level, capacity, and disk status.

You can use the right-click menu to repair, add, or delete disks.

FortiMail/FortiWeb logging and reporting support

FortiManager v5.0 Patch Release 3 introduces FortiMail and FortiWeb logging and reporting support. ADOMs must be enabled on FortiManager before these devices can be added. FortiMail and FortiWeb are log triggered devices. Once configured to log to the FortiManager they will be displayed in the unregistered device list. Upon promoting the device to the DVM table, it will be added to the respective default ADOM.



FortiMail and FortiWeb devices cannot be manually added using the Add Model Device wizard.



FortiMail and FortiWeb devices have specific charts and datasets for report generation.

ADOM for FortiCarrier

FortiGate and FortiCarrier devices can no longer be grouped into the same ADOM in v5.0 Patch Release 3. FortiCarrier devices should be grouped into a dedicated FortiCarrier ADOM.

Drill Down tab

The *Drill Down* tab allows you to generate ad-hoc graphical views of traffic, web, email, and threat activity on an individual FortiGate device, VDOM, or log array.

Event Management tab

In Event Management you can configure events based on logging filters. You can select to send the event to an email address, SNMP server, or syslog server. Events can be configured per device or per log array. You can create events for FortiGate, FortiCarrier, FortiMail, and FortiWeb devices.

Event Management replaces Alert Events.

FortiManager VM support for Microsoft Hyper-V Server

FortiManager VM now supports Microsoft Hyper-V Server 2008 and 2012 virtualization environments.

Import and export report templates

This release adds the ability to import and export report templates. A report template created on one FortiManager device can be exported and imported into another FortiManager device.

RTM profiles

RTM profiles have been removed in FortiManager v5.0 Patch Release 3. You can use the new Drill Down feature to gather detailed information on managed devices and log arrays. Drill down includes traffic, web, email, and threat activity.

Vertical view

Vertical view of devices in the Device Manager tab has been removed in FortiManager v5.0 Patch Release 3.

Summary of enhancements

The following is a list of enhancements in FortiManager v5.0 Patch Release 3:

- ADOM revisions
- Provisioning profile updates
- Certificate Templates menu
- Policy drag & drop extensions
- PKI administrative users
- Display options reorganization
- Device Manager improvements for VDOM listing
- Drill Down tab
- Event Management tab

- FortiManager VM support for Microsoft Hyper-V Server
- Configure up to 10 trusted hosts
- FortiMail and FortiWeb support
- RAID Management menu
- Assign a global policy package to a specific policy
- FortiAP improvements
- Extended the usage of address search

FortiManager v5.0 Patch Release 2

FortiManager v5.0 Patch Release 2 includes the following new features and enhancements. Always review all sections in the *FortiManager Release Notes* prior to upgrading your device.



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

Log arrays

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

After creating a log array, only new logs will be populated into this array. Older logs will remain on the device. To collect older logs, you will need to build the array database. Use the following CLI command to build the array database:

```
execute sql-local rebuild-device <log array device ID>
```

The SQL logs for the members of the log array will be rebuilt. To verify that the array rebuild was successful, select the *Log View* tab to view the log array and logs.



Executing this command will not reboot the FortiManager device.



Fortinet recommends configuring log arrays prior to deploying the FortiManager into production. When adding and deleting log arrays, you will need to rebuild the database to view older logs.

Summary of enhancements

The following is a list of enhancements in FortiManager v5.0 Patch Release 2:

- ADOM revisions
- Device tab customization
- FortiGuard service management
- *Policy & Object* menu organization improvements
- Search improvements
- XML API provisioning improvements

FortiManager v5.0 Patch Release 1

FortiManager v5.0 Patch Release 1 includes the following new features and enhancements. Always review all sections in the *FortiManager Release Notes* prior to upgrading your device.



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

Summary of enhancements

The following is a list of enhancements in FortiManager v5.0 Patch Release 1:

- Added a JSON API to rename a policy package or folder
- FAP-112B and FAP-320B support
- FortiCarrier VM support
- FortiClient software and signature updates support
- Merged interface and zone pages in the *Device Manager*
- *Policy & Objects* dual pane enhancements

FortiManager v5.0.0

FortiManager v5.0.0 includes the following new features and enhancements. Always review all sections in the *FortiManager Release Notes* prior to upgrading your device.



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

Device manager layout

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

The *Device Manager* tab has the following changes:

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

ADOM properties

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

ADOM properties include:

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

Device dashboard

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

The widgets have changed as follows:

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

Policy package status

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

Device profiles

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

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

Device profiles supports the following settings:

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

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

Installation considerations

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

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

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

Extend workspace to entire ADOM

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

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

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

Quick install

You can right-click on the *Policy Config Status* column icon to perform a quick reinstallation of a policy package without launching the *Install Wizard*. The content menu is disabled when the policy package is already in synchronization. You can also right-click on *Config Status* if the device is out of synchronization to install any device setting changes. This will only affect the settings for the selected device. In FortiManager v5.0.0 or later you can perform a quick install for multiple devices.

Bind zone to an address

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

Policy & Objects dual pane

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

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

The following features are available for drag and drop:

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

Web-based Manager improvements have been made to the policy table.

Policy package

You can create the following types of local domain policies/identity policies: Policy, Central NAT, IPv6 Policy, DOS Policy.

Objects

Configurable objects include the following: Zone, Firewall Objects, UTM Objects, User & Device, WAN Opt, Dynamic Objects, CA Certificates, Tag Management.

Policy package granularity

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

Global settings include: System Settings, Administrator Domain, Global Policy Packages, Global Objects, and Assignment.

ADOM settings include: Add/Delete Devices/Groups, Install to Devices, Retrieve Configuration from Devices, Terminal Access, Consistency Check, Device Manager, Manage Device Configuration, Policy Package, Policy Objects, and VPN Manager.

Other settings include: Log Viewer and Report Viewer.

New administrators

When creating a new administrator, you can assign a default or custom administrator profile, and specify ADOM and policy package access.

Reports tab

FortiManager now includes an SQL-based *Reports* tab, similar to FortiAnalyzer.

Report templates

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

Go to *Reports* > *[ADOM]* > *Reports*, to configure report templates and to view report calendars. Use the right-click menu on the tree menu to create a new template or report schedule, and to view historical reports.

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

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

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

You can create schedules for reports and view the schedule either as a list or in calendar format. You can download any previously generated reports from either the list view or calendar view.

Reports allows you to view all reports that have been generated on the FortiManager system. It displays the report name, date and time that the report was generated, and the device type.

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

Advanced

The *Advanced* section allows you to view and configure charts, datasets, output profiles, and languages.

Endpoint management

In version 5.0, FortiClient endpoint agent configuration and management are now handled by the FortiGate Endpoint Control feature. You can configure your FortiGate device to discover new devices on your network, enforce FortiClient registration, and deploy a pre-configured endpoint profile to connected devices. This feature requires a FortiGate device running FortiOS v5.0.0 or later.

Advanced features improvements

JSON API improvements

The following improvements have been made to the JSON API:

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

Script Web-based Manager

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

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

Web portal developer SDK improvements

A new Web Portal Developer tools site has been created. This site is restricted to customers that have purchased the SDK SKU, and will host all of the SDK materials.

XML API improvements

The following improvements have been made to the XML API:

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

High Availability takeover without reboot

In FortiManager v4.0 MR3, when a HA slave was promoted a reboot was required, This behavior has changed so that a reboot is not required when the slave is promoted to master.

IPv6 administration

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

Single interface zones

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

This feature has two parts:

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

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

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

Summary of enhancements

The following is a list of enhancements in FortiManager v5.0.0:

- Added the ability to configure SSL VPN portals
- Added the ability to postpone the promotion of selected unregistered devices
- Administrative domain mode - global view
- Assign and install global policy packages
- Bind a zone to an address
- Configure device profiles
- Configuration status indicator that the FortiGate configuration was auto-updated
- *Device Import Wizard* improvements for all VDOMs
- Device Manager module layout improvements
- Extend workspace to entire ADOM

  Lock ADOMs to prevent other administrators from making changes.

  This feature is available in the *Device Manager* and *Policy & Objects* modules.
- FortiManager IPv6 support
- FortiOS SSL VPN profile management
- FortiToken activation and monitoring

  Query, activate, and monitor FortiTokens associated to a FortiGate device directly from the FortiManager Web-based Manager.
- Global view mode
- High Availability slave notification in Web-based Manager
- High Availability takeover without reboot
- Import objects that are not used by a firewall policy
- IPv6 support
- JSON API improvements
- Log viewer module
- Notification of High Availability slave status
- Policy & Objects module dual pane layout
- Policy package granularity for administrator access

  The admin profile configuration has become more granular. You can specify the access level the administrator is granted at a Global, and ADOM level.
- Policy package status

- Quick install option
- Reports module and template

  Select the Reports tab to configure device reports. You can customize report charts. You can schedule reports to run against specific devices and device groups.
- SCP+ certificate for configuration backup
- Web-based script manager improvements
- Single interface zones

  You can now configure single interface zones and non-single interface zones.
- Support the FortiOS object list
- User accepted auto-sync
- XML API extension for global zone

Fortinet Management Theory

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

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

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

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

Key features of the FortiManager system

Configuration revision control and tracking

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

Centralized management

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

Administrative domains

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

Local FortiGuard service provisioning

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

Firmware management

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

Scripting

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

Logging and reporting

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

Fortinet device life cycle management

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

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

Inside the FortiManager system

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

Device Manager tab

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

Policy & Objects tab

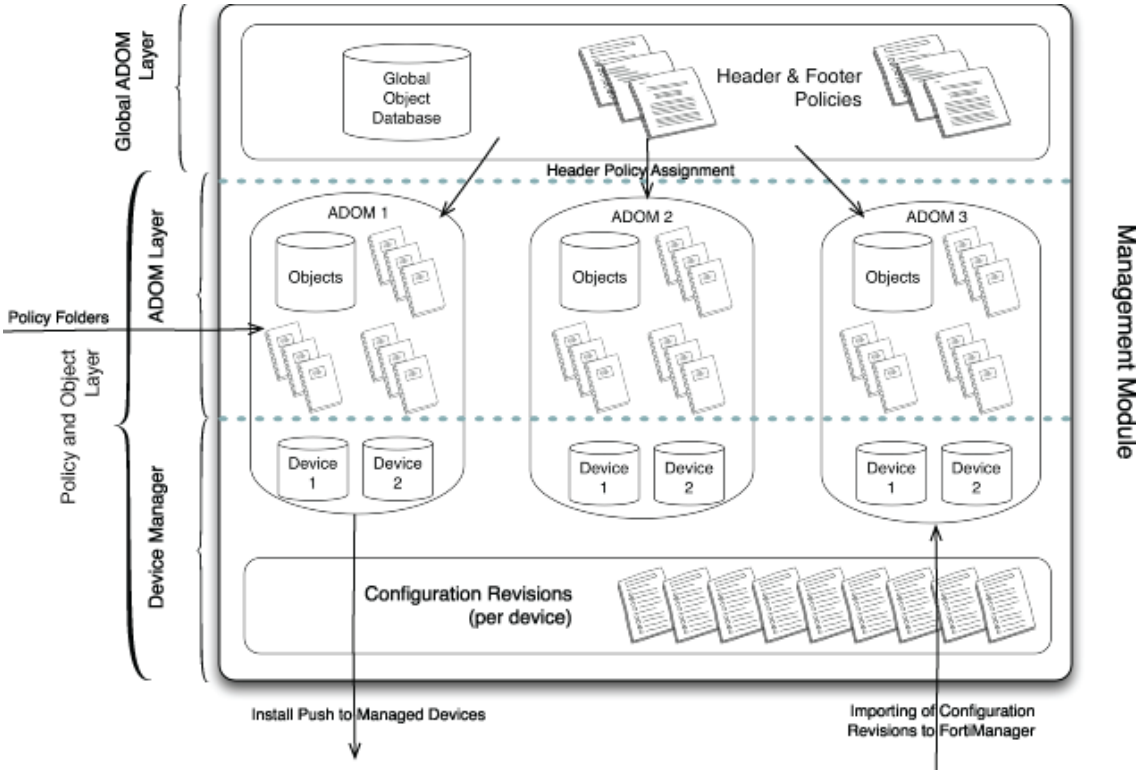
The *Policy & Objects* tab contains all of your global and local policy packages and objects that are applicable to all ADOMs, and configuration revisions.

System Settings tab

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

Inside the FortiManager device manager tab

Figure 1: Management model



Global ADOM layer

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

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

ADOM layer

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

Device manager layer

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

Using the Web-based Manager

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

This section includes the following topics:

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



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

System requirements

Supported web browsers

The following web browsers are supported by FortiManager v5.0 Patch Release 5:

- Internet Explorer versions 9 and 10
- Mozilla Firefox version 24
- Google Chrome version 30

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

Monitor settings for Web-based Manager access

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

Connecting to the Web-based Manager

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

To connect to the Web-based Manager:

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

You can now proceed with configuring your FortiManager unit.



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

For information on enabling administrative access protocols and configuring IP addresses, see "Configuring network interfaces" on page 87.



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 88.

Web-based Manager overview

FortiManager v5.0 Patch Release 5 introduces an improved Web-based Manager layout and tree menu for improved usability. For more information, see "What's New in FortiManager v5.0" on page 22.

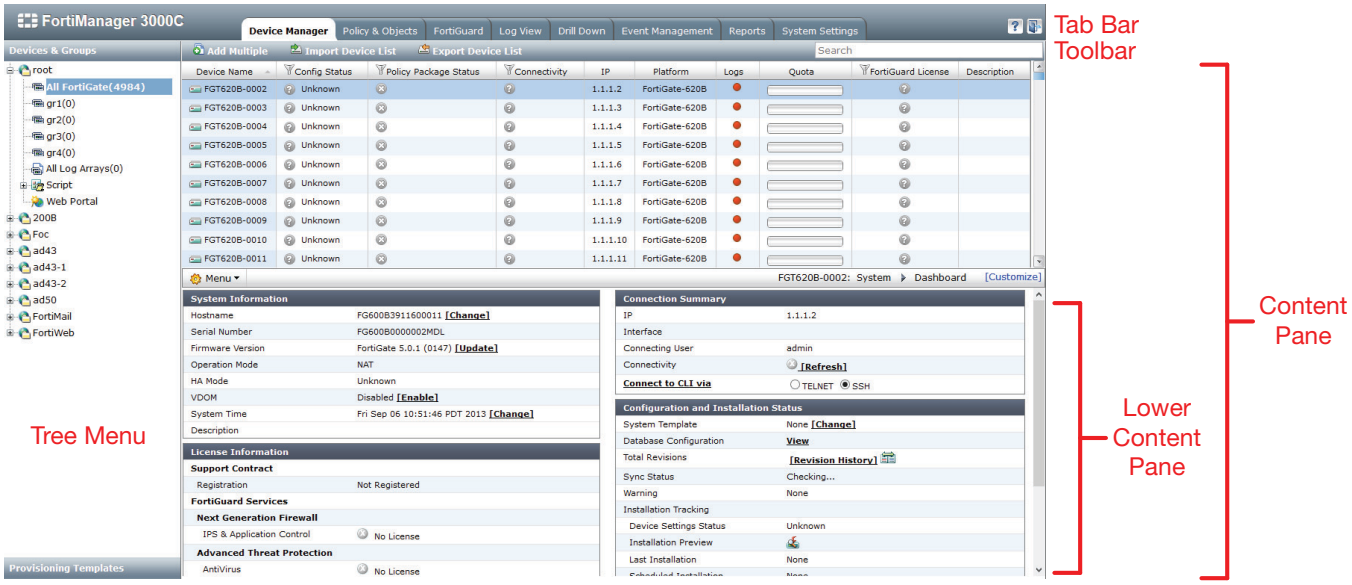
This section describes the following topics:

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

Viewing the Web-based Manager

The five main parts of the FortiManager Web-based Manager are the tree menu, tab bar, navigation pane, toolbar, and right content pane.

Figure 2: Web-based Manager



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

The navigation pane and content pane information displayed to an administrator vary according to the administrator account settings and access profile that have be configured for that user. To configure admin profiles, go to *System Settings* > *Admin* > *Profile*. You can configure the admin profile at both a global and ADOM level with a high degree of granularity in providing read-write, read-only, or restricted access to various Web-based Manager modules. When defining a new administrator, you can further define which ADOMs and policy packages the administrator can access. For more information about administrator accounts and their privileges, see "Admin" on page 92.

When you log in to the FortiManager unit as the `admin` administrator, the Web-based Manager opens to the *Device Manager* tab. You can view all ADOMs in the navigation tree, and ADOM information in the content pane. For more information, see "Device Manager" on page 129.



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

Using the navigation pane

The navigation is organized into a number of tabs.

Table 1: Web-based Manager tabs

Tab	Description
Device Manager	Add and manage devices, view the device information and status, create and manage device groups and manage firewall global policy objects. From this menu, you can also configure the web portal configurations, users, and groups. In the Menu section, you can configure managed devices locally in the FortiManager Web-based Manager. In the Provisioning Templates section, you can configure System Templates, WiFi Templates, Endpoint Templates, and Certificate Templates and assign these templates to specific managed FortiGate and FortiCarrier devices. For more information, see "Device Manager" on page 129.
Policy & Objects	Configure policy packages and objects. When Central VPN Console is enabled for the ADOM, you can create VPN topologies and managed/external gateways. For more information, see "Policy & Objects" on page 278.
FortiGuard	Configure FortiGuard Center settings, package and query server management, and firmware images. For more information, see "FortiGuard Management" on page 443.
Log View	View logs for managed devices. You can display, download, import, and delete logs on this page. For more information, see "Log View" on page 359.
Drill Down	Generate ad-hoc graphical views of traffic, web, email, and threat activity on an individual device, VDOM, or log array. For more information, see "Drill Down" on page 380.
Event Management	Configure and view events for managed log devices. You can view events by severity or by handler. For more information, see "Event Management" on page 383.

Table 1: Web-based Manager tabs

Tab	Description
Reports	Configure report templates, schedules, and output profiles. You can create and test datasets, configure output profiles, and add language support. For more information, see "Reports" on page 396.
System Settings	Configure system settings such as network interfaces, administrators, system time, server settings, and widgets and tabs. From this menu, you can also perform maintenance and firmware operations. For more details on using this menu, see "System Settings" on page 57.



The navigation pane is dependent on administrator profile settings.

Configuring Web-based Manager settings

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

This section includes the following topics:

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

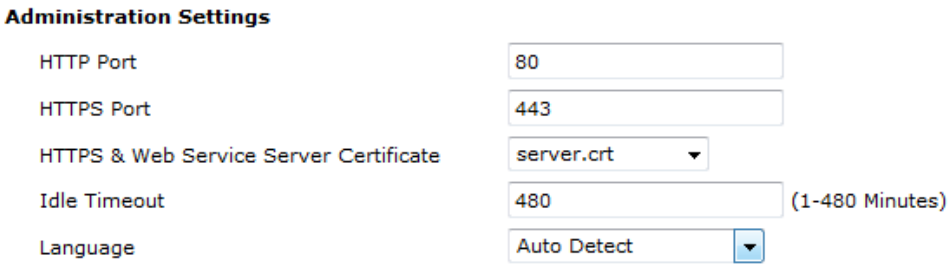
Changing the Web-based Manager language

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

To change the Web-based Manager language:

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

Figure 3: Administration settings



Administrative access

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

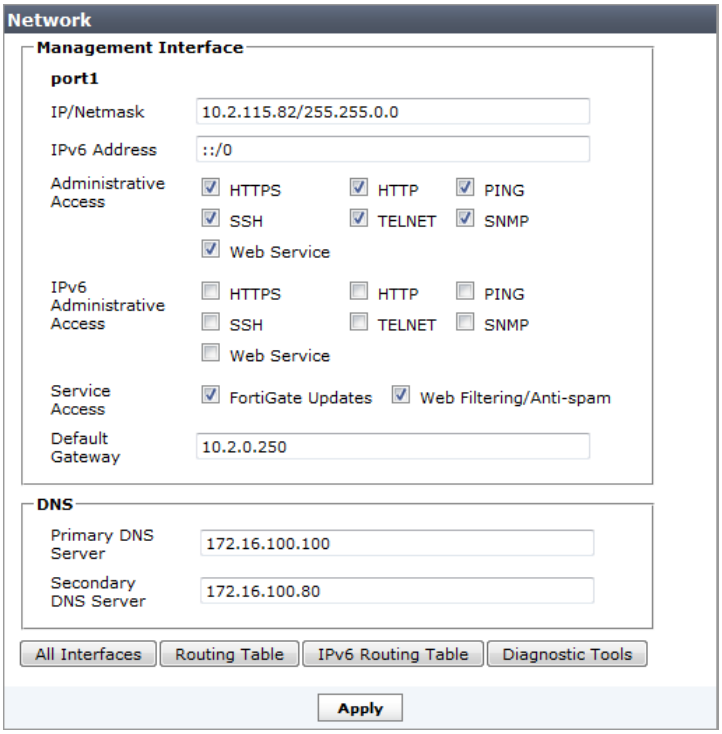
Administrative access can be configured in IPv4 or IPv6 and includes the following settings:

HTTPS	PING	TELNET	Web Service
HTTP	SSH	SNMP	

To change administrative access to your FortiManager system:

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

Figure 4: Management Interface page



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

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

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

Restricting Web-based Manager access by trusted host

To prevent unauthorized access to the Web-based Manager you can configure administrator accounts with trusted hosts. With trusted hosts configured, the admin user can only log into the Web-based Manager when working on a computer with the trusted host as defined in the admin account. You can configure up to ten trusted hosts per administrator account. See "Administrator" on page 94 for more details.

Changing the Web-based Manager idle timeout

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

To change the Web-based Manager idle timeout:

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

Other security considerations

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

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

Reboot and shutdown of the FortiManager unit

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

To reboot the FortiManager unit:

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

```
execute reboot
```

To shutdown the FortiManager unit:

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

```
execute shutdown
```

Administrative Domains

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

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

ADOMs are not enabled by default, and enabling and configuring the domains can only be performed by the `admin` administrator. For more information, see "Enabling and disabling the ADOM feature" on page 49.

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

This section includes the following topics:

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

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

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

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



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

Enabling and disabling the ADOM feature

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

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

ADOMs must be enabled to support FortiMail and FortiWeb logging and reporting. When a FortiMail or FortiWeb device is promoted to the DVM table, the device is added to their respective default ADOM and will be visible in the left tree menu.

FortiGate and FortiCarrier devices cannot be grouped into the same ADOM. FortiCarrier devices are added to a specific default FortiCarrier ADOM.

To enable the ADOM feature:

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

Figure 5: Enabling ADOMs

System Information	
Host Name	FMG-VM64-HV [Change]
Serial Number	FMG-VM0A11000137
Platform Type	FMG-VM64-HV
HA Status	Standalone
System Time	Mon Oct 28 13:25:05 PDT 2013 [Change]
Firmware Version	v5.0-build0254 131025 (Interim) [Update]
System Configuration	Last Backup:Mon Oct 28 13:22:26 2013 [Backup] [Restore] [System Checkpoint]
Current Administrators	admin [Change Password] /6 in Total [Detail]
Up Time	3 days 1 hour 27 minutes 21 seconds
Administrative Domain	Enabled [Disable]

To disable the ADOM feature:

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

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

ADOM modes

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

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

Switching between ADOMs

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

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

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

Normal mode ADOMs

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

Backup mode ADOMs

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

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

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

ADOM versions

ADOMs can concurrently manage FortiGate units running both FortiOS version 4. MR3 and 5.0, allowing devices running these versions to share a common database. This allows you to continue to manage an ADOM as normal while upgrading the devices within that ADOM.



It is recommended that this feature be used only to facilitate upgrading to new firmware and that ADOMs are not regularly run in this mode.

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

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

1. Make sure that the FortiManager unit is upgraded to a version that supports this feature (v5.0 Patch Release 5).
2. In the ADOM, upgrade one of the FortiGate units to FortiOS 5.0, and then resynchronize the device.

   All the ADOM objects, including Policy Packages, remain as v4.0 MR3.
3. Upgrade the rest of the FortiGate units in the ADOM to version 5.0 firmware.
4. Upgrade the ADOM to v5.0. See "Upgrading an ADOM" on page 54 for more information.

   All of the database objects will be converted the v5.0 format, and the Web-based Manager content for the ADOM will change to reflect the v5.0 features and behavior.



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

Managing ADOMs

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

To configure and manage ADOMs, go to the *Device Manager* tab, or to *System Settings* > *All ADOMs*. See "All ADOMs" on page 79 for more information.

Extend workspace to entire ADOM

When concurrent ADOM access is disabled, administrators are able to lock the ADOM. A right-click menu option has been added to allow you to lock/unlock ADOM access; see "Locking an ADOM" on page 56. The ADOM lock status is displayed by a lock icon to the left of the ADOM name.

The lock status is as follows:

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

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

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

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



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

Concurrent ADOM access

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

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



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

To enable ADOM locking and disable concurrent ADOM access:

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

To disable ADOM locking and enable concurrent ADOM access:

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

Adding an ADOM

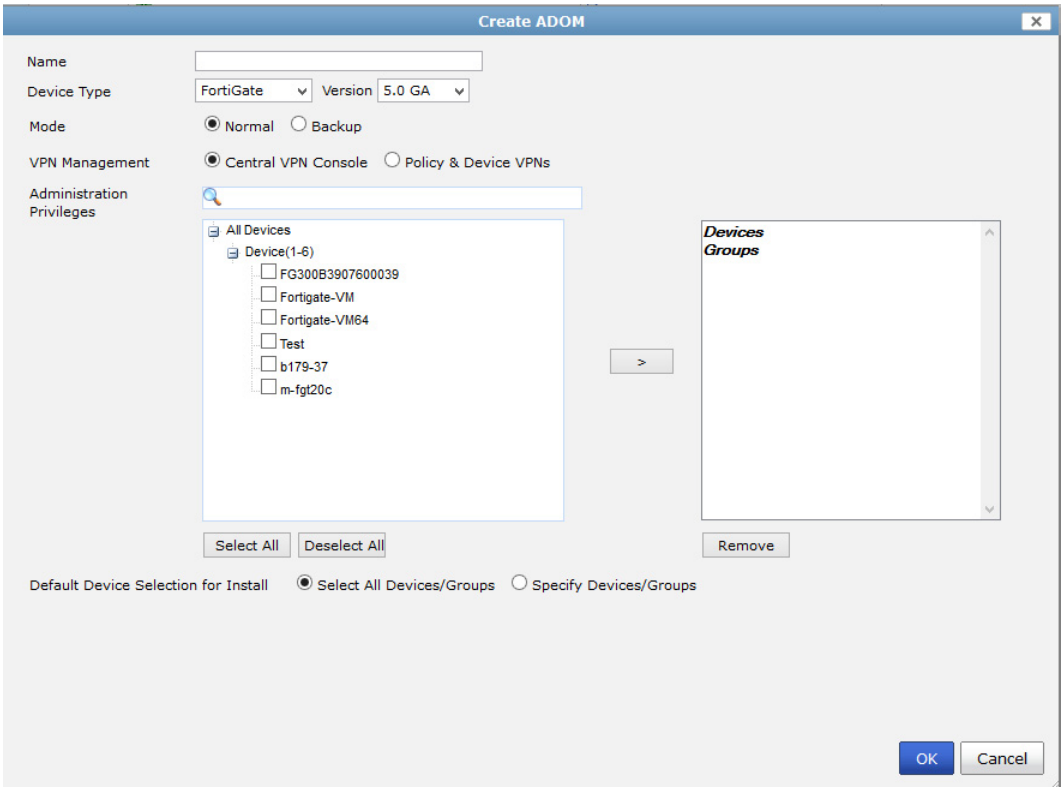
To add an ADOM, you must be logged in as the `admin` administrator. You must also first enable administrative domains in the Web-based Manager; see “To enable the ADOM feature:” on page 49.

To create an ADOM

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

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

Figure 6: Create ADOM dialog box



2. Enter the following information:

Name	Enter a name that will allow you to distinguish this ADOM from your other ADOMs. Note: ADOM names must be unique.
Device Type	Select either FortiGate or FortiCarrier from the drop-down menu. Other devices types are added to their respective default ADOM upon registering with FortiManager.
Version	Select the version of FortiGate devices in the ADOM. FortiManager v5.0 supports FortiOS v5.0, v4.0 MR3, and v4.0 MR2. For information on supported device firmware version, see the *FortiManager v5.0 Patch Release 5 Release Notes*.

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*. When *Central VPN Console* is selected, the *VPN Console* menu item will be visible under the *Policy & Objects* tab. You can configure VPN topologies and managed/external gateway objects.
Device	Select members from the *Available member* list and transfer them to the *Selected member* list to assign the devices to the ADOM.
Default Device Selection for Install	Select either *Select All Devices/Groups* or *Specify Devices/Groups*.

3. Select *OK* to create the ADOM.

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

Deleting an ADOM

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

To delete an ADOM

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



The root ADOM cannot be deleted.

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

Upgrading an ADOM

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

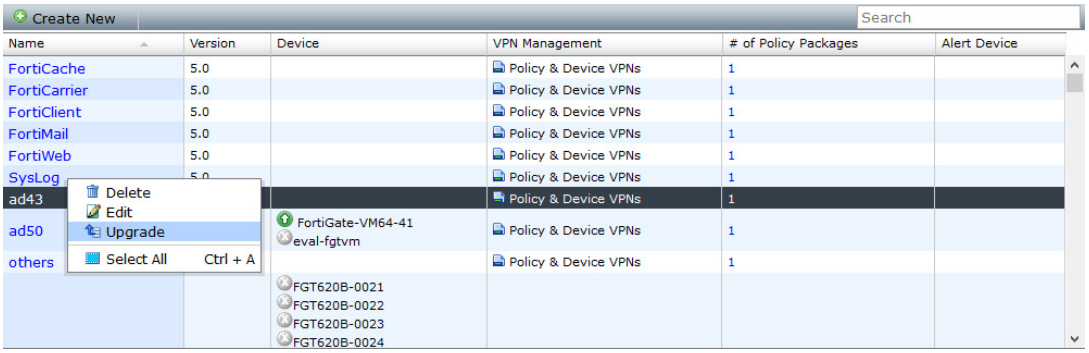


An ADOM can only be upgraded after all the devices within the ADOM have been upgraded. See "ADOM versions" on page 51 for more information.

To upgrade an ADOM:

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

Figure 7: Upgrade an ADOM



If the ADOM has already been upgraded to the latest version, this option will not be available.

3. Select *OK* in the confirmation dialog box to upgrade the device.

   If all of the devices within the ADOM are not already upgraded to v5.0, the upgrade will be aborted and a warning dialog box will be shown. Select *OK* in the dialog box, upgrade the remaining devices within the ADOM, and return to step 1 to try upgrading the ADOM again.

Assigning devices to an ADOM

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

To assign devices to an ADOM:

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

   The *Edit ADOM* dialog box will open.

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

   If the administrative device mode is *Advanced*, you can add separate FortiGate VDOMs to the ADOM as well as FortiGate units. For more information see "ADOM device modes" on page 55.

3. When done, select *OK*. The selected devices appear in the device list for that ADOM.



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

ADOM device modes

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

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

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

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

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

Assigning administrators to an ADOM

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



By default, when ADOMs are enabled, existing administrator accounts other than `admin` are assigned to the `root` domain, which contains all devices in the device list. For more information about creating other ADOMs, see "Assigning devices to an ADOM" on page 55.

To assign an administrator to an ADOM:

1. Log in as `admin`.

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



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

Locking an ADOM

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

To lock an ADOM from the Device Manager tab:

Right-click on the ADOM name in the tree menu and select *Lock* from the pop-up menu.

The ADOM will now be locked, allowing you to make changes to it, and preventing other administrators from making any changes, unless lock override is enabled.

To lock an ADOM from the Policies and Objects tab:

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

   The ADOM will now be locked, allowing you to make changes to it, and preventing other administrators from making any changes, unless lock override is enabled.

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.

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

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

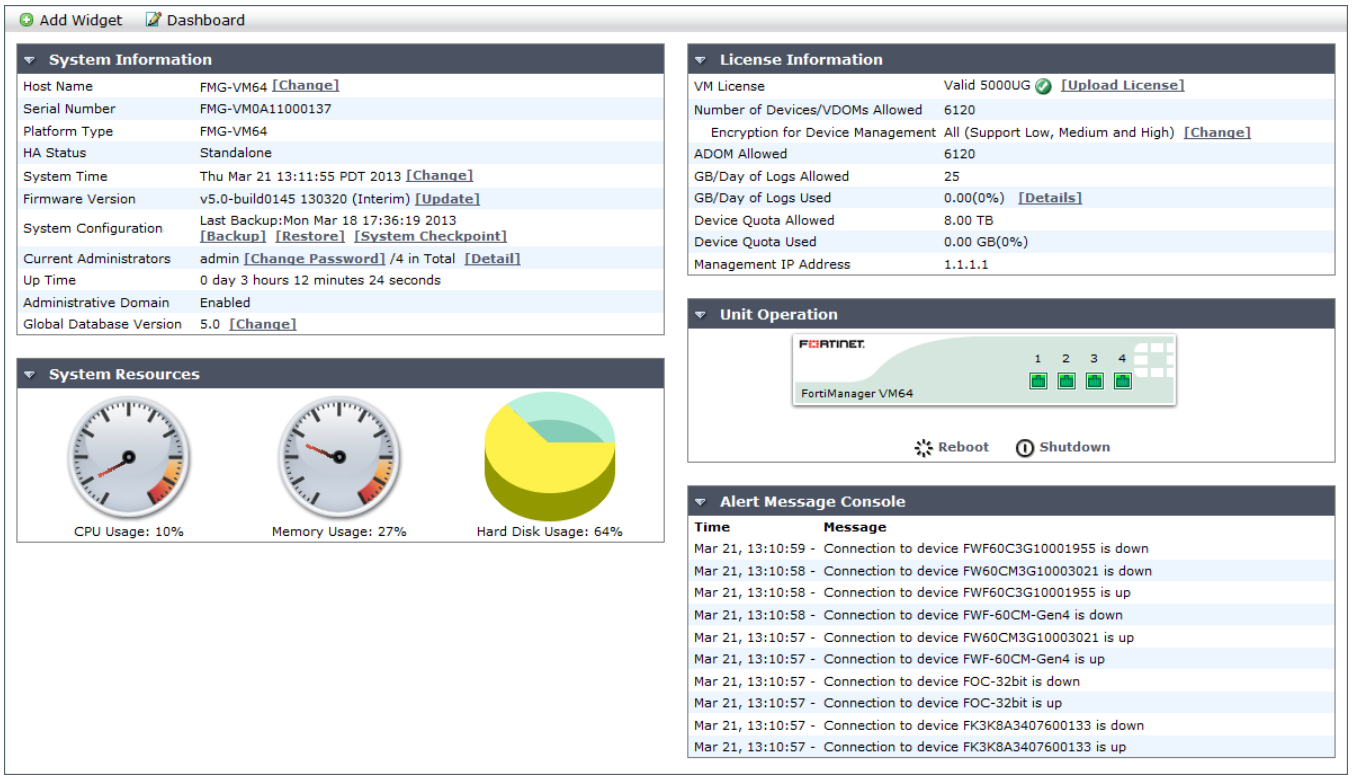
Task Monitor	The Task Monitor page allows you to view the status of the tasks that you have performed.
Advanced	Select to configure mail server settings, remote output, SNMP, meta field data and other advanced settings. • SNMP v1/v2c • Mail Server • Syslog Server • Meta Fields • Device Log Settings • Advanced Settings

Dashboard

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

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

Figure 8: 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 "System Information widget" on page 62. From this widget you can also manually update the FortiManager firmware to a different release. For more information, see "Firmware images" on page 468.
License Information	Displays the devices being managed by the FortiManager unit and the maximum numbers of devices allowed. For more information, see "License Information widget" on page 72.
Unit Operation	Displays status and connection information for the ports of the FortiManager unit. It also enables you to shutdown and restart the FortiManager unit or reformat a hard disk. For more information, see "Unit Operation widget" on page 74.

System Resources	Displays the real-time and historical usage status of the CPU, memory and hard disk. For more information, see “System Resource widget” on page 70.
Alert Message Console	Displays log-based alert messages for both the Fortinet unit itself and connected devices. For more information, see “Alert Messages Console widget” on page 74.
CLI Console	Opens a terminal window that enables you to configure the FortiManager unit using CLI commands directly from the Web-based Manager. This widget is hidden by default. For more information, see “CLI Console widget” on page 75.
Log Receive Monitor	Displays a real-time monitor of logs received. You can select to view data per device or per log type. For more information, see “Log Receive Monitor widget” on page 76.
Logs/Data Received	Displays real-time or historical statistics of logs and data received. For more information, see “Logs/Data Received widget” on page 78.
Statistics	Displays statistics for logs and reports. For more information, see “Statistics widget” on page 79.

Customizing the dashboard

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

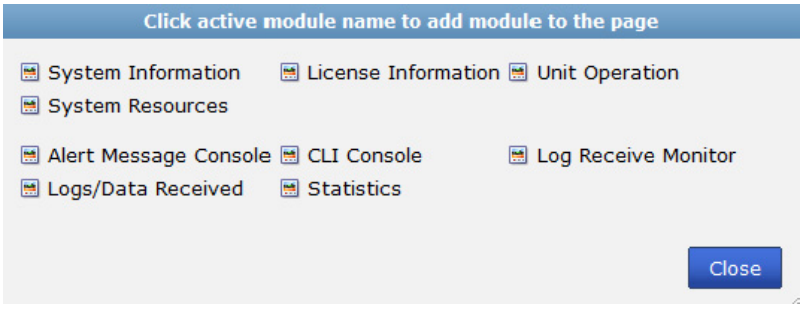
To move a widget

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

To add a widget

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

Figure 9: 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 reset the dashboard

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

To see the available options for a widget

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

Figure 10:A minimized widget



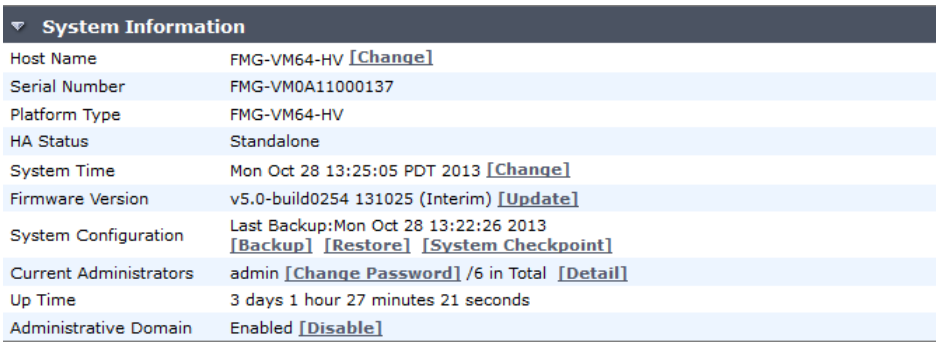
The following options are available:

Show/Hide arrow	Display or minimize the widget.
Widget Title	The name of the widget.
More Alerts	Show the *Alert Messages* dialog box. This option appears only on the Alert Message Console widget.
Edit	Select to change settings for the widget. This option appears only on the System Resources, Alert Message Console, Logs/Data Received, and Log Receive Monitor widgets.
Detach	Detach the CLI Console widget from the dashboard and open it in a separate window. This option appears only on the CLI Console widget.
Refresh	Select to update the displayed information.
Close	Select to remove the widget from the dashboard. You will be prompted to confirm the action. To add the widget, select *Widget* in the toolbar and then select the name of the widget you want to show.

System Information widget

The system dashboard includes a System Information widget, shown in Figure 11, which displays the current status of the FortiManager unit and enables you to configure basic system settings.

Figure 11: System Information widget



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

Host Name	The identifying name assigned to this FortiManager unit. Select *[Change]* to change the host name. For more information, see "Changing the host name" on page 63.
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 470.
System Time	The current time on the FortiManager internal clock. Select *[Change]* to change system time settings. For more information, see "Configuring the system time" on page 64.
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 65.

System Configuration	The date of the last system configuration backup. The following actions are available: • Select *[Backup]* to backup the system configuration to a file; see "Backing up the system" on page 66. • Select *[Restore]* to restore the configuration from a backup file; see "Restoring the configuration" on page 67. • Select *[System Checkpoint]* to revert the system to a prior saved configuration; see "Creating a system checkpoint" on page 68.
Current Administrators	The number of administrators that are currently logged in. The following actions are available: • Select *[Change Password]* to change your own password. • Select *[Detail]* to view the session details for all currently logged in administrators. See "Monitoring administrator sessions" on page 92 for more information.
Up Time	The duration of time the FortiManager unit has been running since it was last started or restarted.
Administrative Domain	Displays whether ADOMs are enabled. Select *[Enable/Disable]* to change the Administrative Domain state. See "Enabling and disabling the ADOM feature" on page 49.
Global Database Version	Displays the current Global Database version. Select *[Change]* to change the global database version.

Changing the host name

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

- It appears in the *System Information* widget on the *Dashboard*. For more information about the *System Information* widget, see "System Information widget" on page 62.
- It is used in the command prompt of the CLI.
- It is used as the SNMP system name. For information about SNMP, see "SNMP v1/v2c" on page 115.

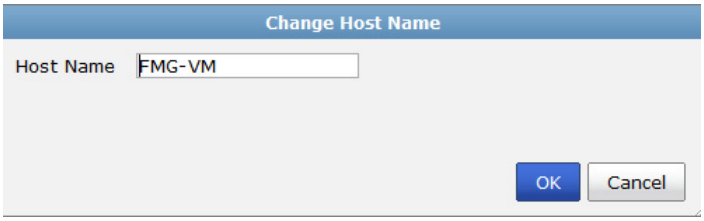
The System Information widget and the `get system status` CLI command will display the full host name. However, if the host name is longer than 16 characters, the CLI and other places display the host name in a truncated form ending with a tilde (~) to indicate that additional characters exist, but are 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* > *Dashboard*.
2. In the *System Information* widget, next to the *Host Name* field, select *[Change]*.

   The *Change Host Name* dialog box opens.

Figure 12: 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.

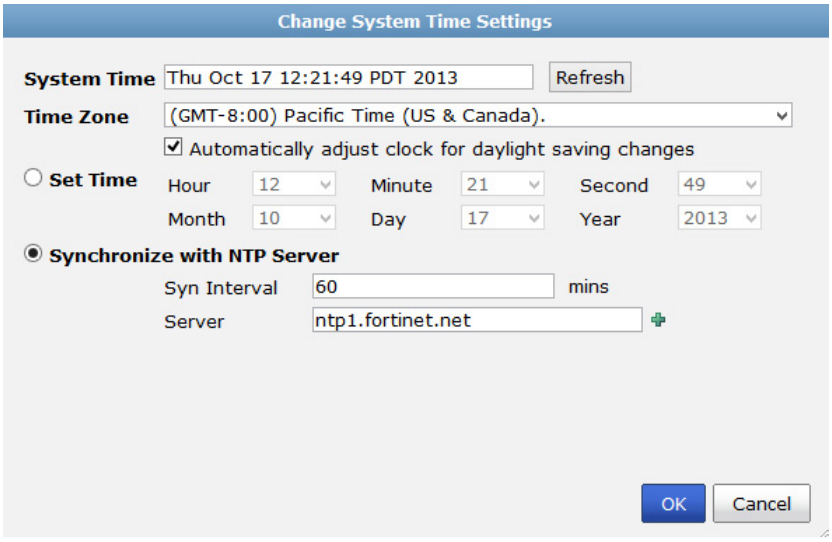


For many features to work, including scheduling, logging, and SSL-dependent features, the Fortinet system time must be accurate.

To configure the date and time

1. Go to *System Settings* > *General* > *Dashboard*.
2. In the *System Information* widget, in the *System Time* field, select *Change*. The *Change System Time Settings* dialog box appears, see Figure 13.

Figure 13: Time Settings dialog box



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

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

4. Select *OK* to apply your changes.

Updating the system firmware

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



Back up the configuration and database before changing the firmware of your Fortinet unit. Changing the firmware to an older or incompatible version may reset the configuration and database to the default values for that firmware version, resulting in data loss. For information on backing up the configuration, see "Backing up the system" on page 66.



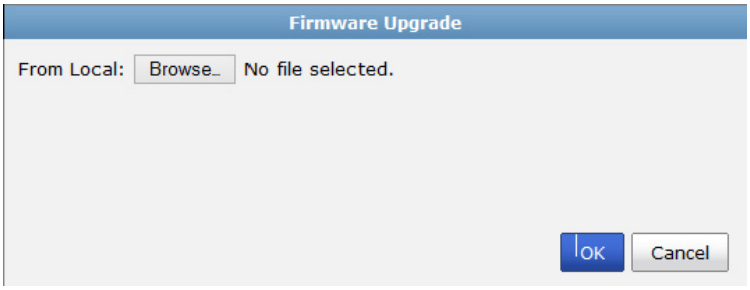
Before you can download firmware updates for your Fortinet unit, you must first register your Fortinet unit with Customer Service & Support. For details, go to https://support.fortinet.com/ or contact Customer Service & Support.

To manually update the Fortinet firmware:

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

   The Firmware Upgrade window opens.

Figure 14: Firmware upgrade



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

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

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

   If you changed the firmware to an earlier version whose configuration is not compatible, you may need to do first-time setup again. For instructions, see the *FortiManager QuickStart Guide* for your unit.
8. Update the vulnerability management engine and definitions. For details, see "FortiGuard Management" on page 443.



Installing firmware replaces the current network vulnerability management engine with the version included with the firmware release that you are installing. After you install the new firmware, make sure that your vulnerability definitions are up-to-date. For more information, see "FortiGuard Management" on page 443.

The FortiManager firmware can also be updated through the FDN. For more information, see "Firmware images" on page 468 of the "FortiGuard Management" chapter.

Backing up the system

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

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

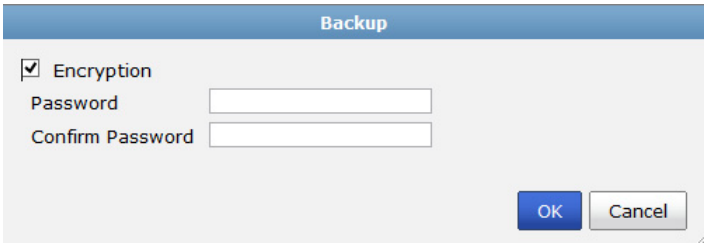
Fortinet recommends backing up all configuration settings from your FortiManager unit before upgrading the FortiManager firmware.

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

To back up the FortiManager configuration:

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

Figure 15: 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 the encryption check box is selected.)
Confirm Password	Re-enter the password to confirm it.

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

Restoring the configuration

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

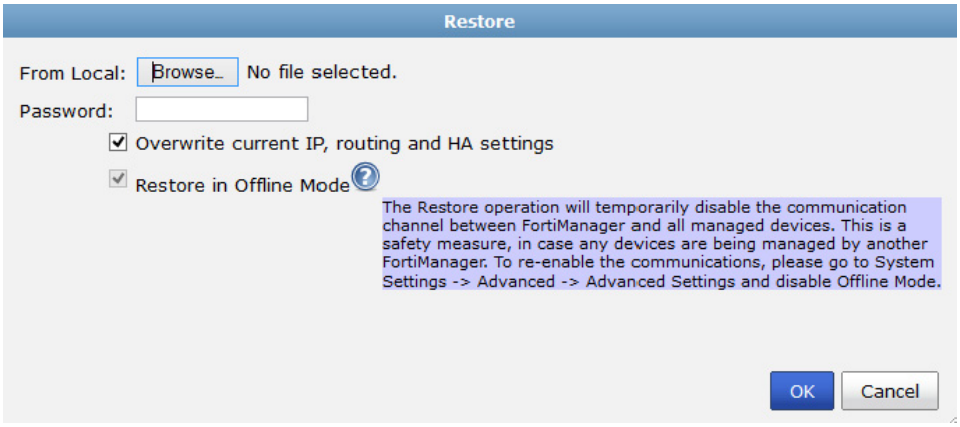


The restore operation will temporarily disable the communication channel between FortiManager and all managed devices. This is a safety measure, in case any devices are being managed by another FortiManager. To re-enable the communication, please go to *System Settings* >*Advanced* >*Advanced Settings*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

To restore the FortiManager configuration:

1. Go to *System Settings* > *Dashboard*.
2. In the System Information widget, under *System Configuration*, select *[Restore]*. The *Restore* dialog box appears; see Figure 16.

Figure 16: Restore dialog box



3. Configure the following settings and select OK.

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

Creating a system checkpoint

You can create a system checkpoint backup to capture a specific configuration. This backup provides a history where the FortiManager and FortiGate units are completely in sync. Should there be a major failure, you can completely revert the network to when it was in working order, and not have to be concerned about which device has which versions of the firmware installed and so on. These are, in essence, snapshots of your Fortinet managed network system.

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

A system checkpoint backup includes:

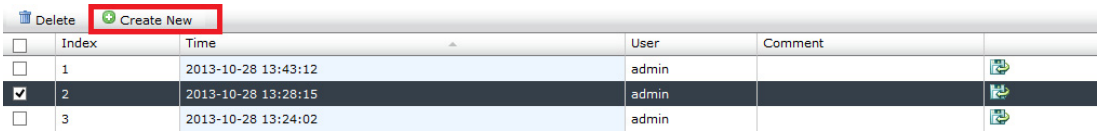
- the current configuration file from each managed device
- the entire system configuration of the FortiManager unit.

To create a system checkpoint:

1. Go to *System Settings* > *Dashboard*.
2. In the System Information widget, under *System Configuration*, select *[System Checkpoint]*.

   The System Checkpoint table opens.

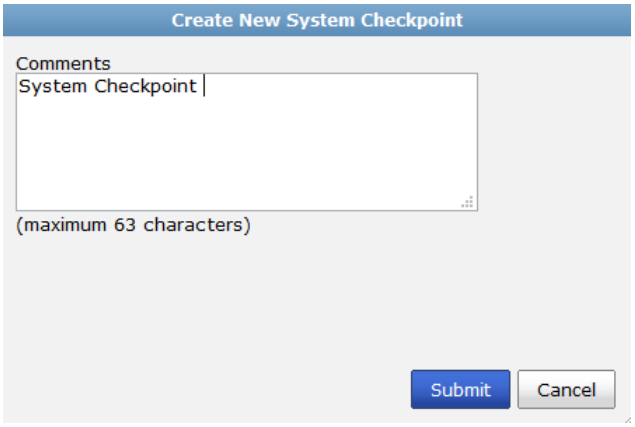
Figure 17: System checkpoint table



3. Select *Create New*.

   The *Create New System Checkpoint* dialog box opens.

Figure 18: Create new system checkpoint



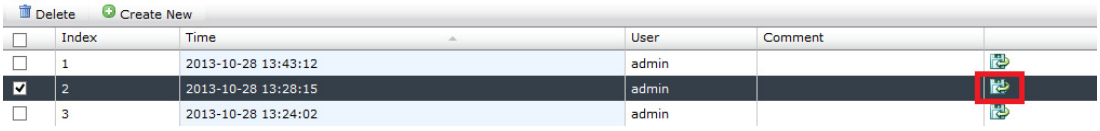
4. In the *Comments* field, enter a description, up to 63 characters, for the reason or state of the backup.
5. Select *Submit*. The system checkpoint task will be run and the checkpoint will be created.

To revert to a system checkpoint:

1. Go to *System Settings* > *Dashboard*.
2. In the System Information widget, under *System Configuration*, select *[System Checkpoint]*.

   The *System Checkpoint* table opens.

Figure 19: System checkpoint table



3. Select the system checkpoint in the table and select the *Revert* icon.
4. A confirmation dialog box will open. Select *OK* to continue.



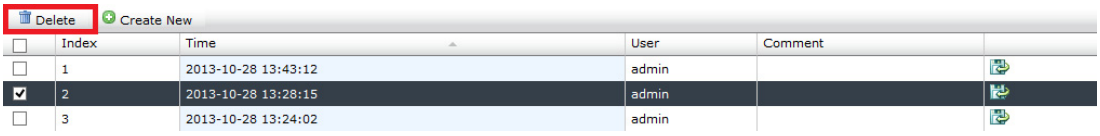
When reverting to a system checkpoint, this FortiManager and all managed FortiGates will reboot.

To delete a system checkpoint:

1. Go to *System Settings* > *Dashboard*.
2. In the System Information widget, under *System Configuration*, select *[System Checkpoint]*.

   The *System Checkpoint* table opens.

Figure 20: System checkpoint table



3. Select the system checkpoint in the table and select the *Delete* in the toolbar.
4. A confirmation dialog box will open. Select *OK* to continue.

System Resource widget

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

Figure 21: System Resource widget (Real Time display)

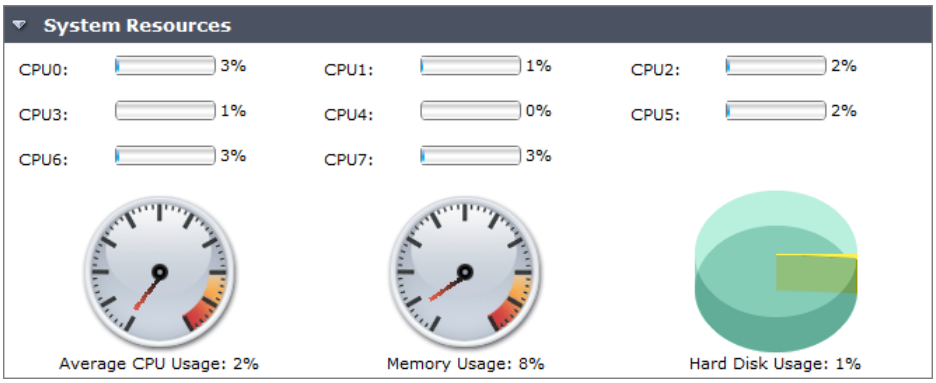
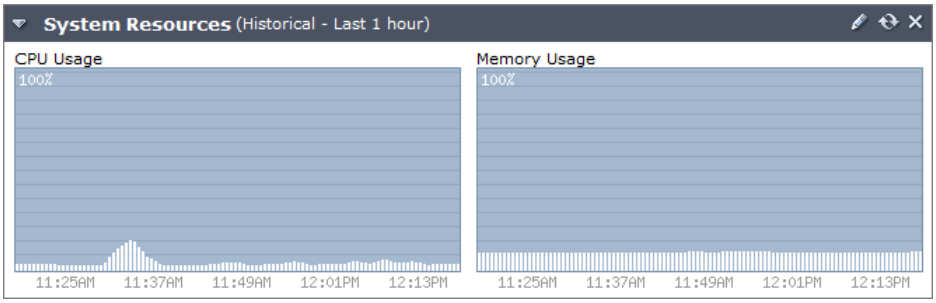


Figure 22: System Resource widget (Historical display)



The following information is displayed on this widget:

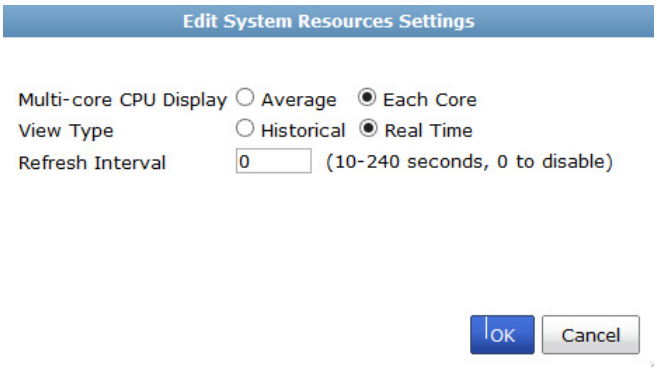
CPU Usage	The current CPU utilization. The Web-based Manager displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the Web-based Manager) is excluded. The average CPU usage can be shown, as well as the usage for each CPU core.
Memory Usage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

Change the system resource widget display settings:

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

   The *Edit System Resources Settings* dialog box appears.

Figure 23: Edit System Resources Settings window



3. You can configure the following settings:

Multi-core CPU Display	To view the resource information for all the cores as an average, from *Multi-core CPU Display*, select *Average*, or, to view individual information for each core, select *Each Core* (the default value).
View Type	To view only the most current information about system resources, from *View Type*, select *Real Time*. This is the default. To view historical information about system resources, from *View Type*, select *History*. To change the time range, from *Time Period*, select one of the following: *Last 10 minutes*, *Last 1 hour,* or *Last 24 hours*.
Refresh Interval	To automatically refresh the widget at intervals, in *Refresh Interval*, type a number between 10 and 240 seconds. To disable the refresh interval feature, type `0`.

4. Select *OK* to apply your settings.

License Information widget

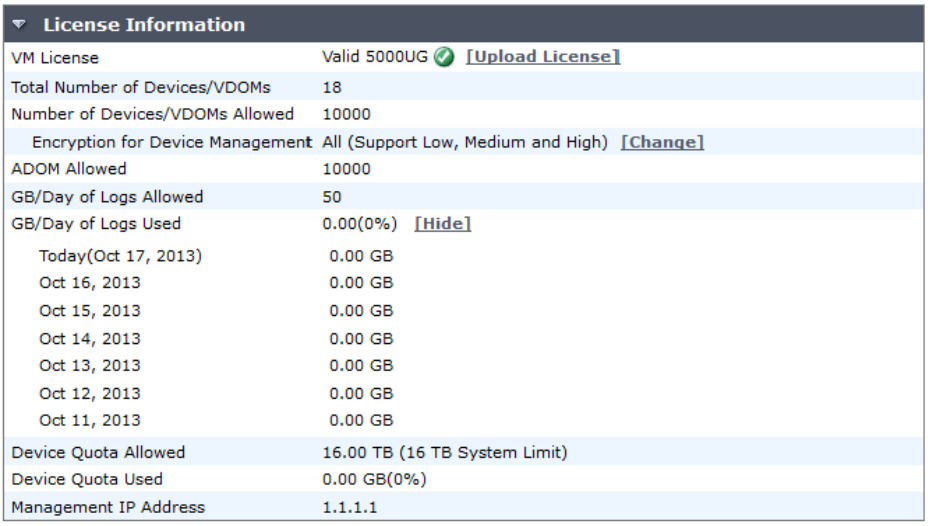
The license information displayed on the dashboard shows, in a single snapshot, the devices being managed by the FortiManager unit and the maximum numbers of devices allowed. The maximums are based on FortiManager system resources.

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



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

Figure 24:VM License Information widget



The following information is displayed in this widget:

VM License	VM license information and status. Select *[Upload License]* to upload a new VM license file. *Note:* This field is only visible for FortiManager VM.
Total Number of Devices/VDOMs	The total number of devices and VDOMs configured on this FortiManager.
Encryption for Device Management	The encryption mode for device management. Select *[Change]* to change the encryption mode. Select one of the following: • All (Support Low, Medium, and High) • Medium (support Medium and High) • High (Support High only)

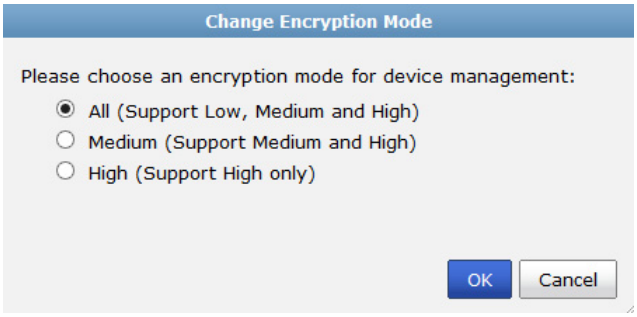
ADOM Allowed	The number of ADOMs allowed to be configured on this FortiManager. The ADOM maximum value is dependent on the FortiManager model.
GB/Day of Logs Allowed	The GB per day of logs allowed for this FortiManager.
GB/Day of Logs Used	The GB per day of logs used for this FortiManager. Select *[Details/Hide]* to view the GB per day of logs used for the previous 6 days.
Device Quota Allowed	The device quota allowed for this FortiManager. *Note:* This field is only visible for FortiManager VM.
Device Quota Used	The device quota used for this FortiManager. *Note:* This field is only visible for FortiManager VM.
Management IP Address	The FortiManager VM management IP address associated with the FortiManager VM license. *Note:* This field is only visible for FortiManager VM. For more information on changing the management IP address, see the *FortiManager VM (VMware) Install Guide*.

To change the encryption mode:

1. In the License Information widget, select *Change* in the *Encryption for Device Management* field.

   The *Change Encryption Mode* dialog box opens.

   Figure 25: Change the encryption mode



2. Select *All*, *Medium*, or *High* for the encryption mode.
3. Select OK to apply the change.

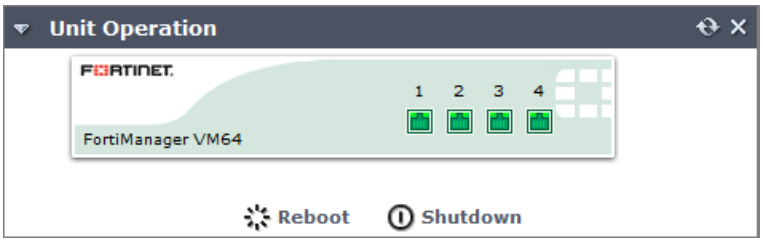
To view the details of the GB/Day of logs used:

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

Unit Operation widget

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

Figure 26: Unit Operation widget



The following information is displayed in this widget

Port numbers (vary depending on model)	The image below the port name indicates its status by its color. Green indicates the port is connected. Grey indicates there is no connection. For more information about a port's configuration and throughput, position your mouse over the icon for that port. You will see the full name of the interface, the IP address and netmask, the status of the link, the speed of the interface, and the number of sent and received packets.
Reboot	Select to restart the FortiManager unit. You are prompted to confirm before the reboot is executed.
Shutdown	Select to shutdown the FortiManager unit. You are prompted to confirm before the shutdown is executed.

Alert Messages Console widget

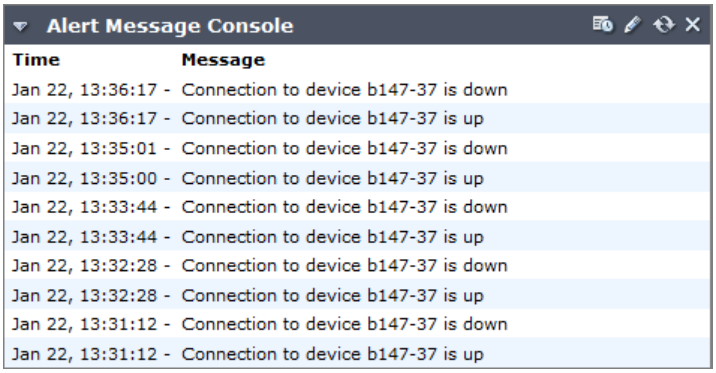
The Alert Message Console widget displays log-based alert messages for both the Fortinet unit itself and connected devices.

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



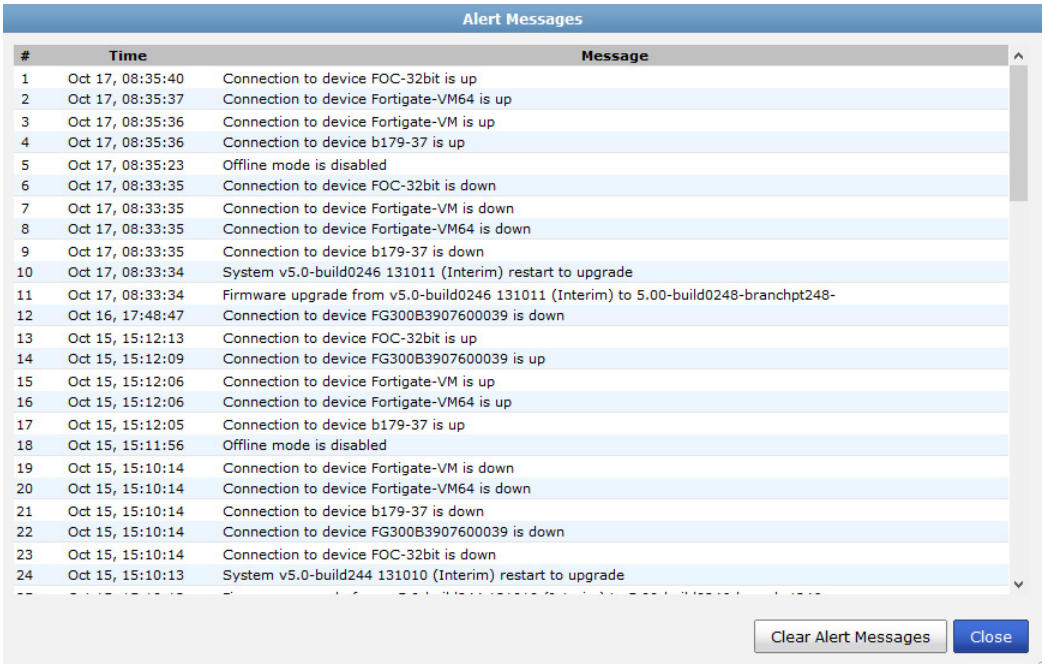
Alert messages can also be delivered by email, syslog, or SNMP.

Figure 27: Alert Message Console widget



The widget displays only the most current alerts. For a complete list of unacknowledged alert messages (see Figure 28), select the *More Alerts* icon in the widget's title bar. A popup window appears. To clear the list, select *Clear Alert Messages*.

Figure 28: List of all alert messages



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

CLI Console widget

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

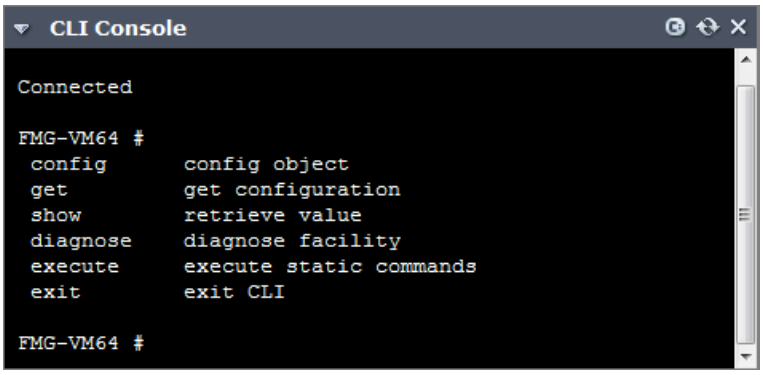


The CLI Console widget requires that your web browser support JavaScript.

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

The command prompt, by default the model number such as `Fortinet-800B #`, contains the host name of the Fortinet unit. To change the host name, see "Changing the host name" on page 63.

Figure 29:CLI Console widget



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

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

Log Receive Monitor widget

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

Figure 30: Log receive monitor widget (log type)

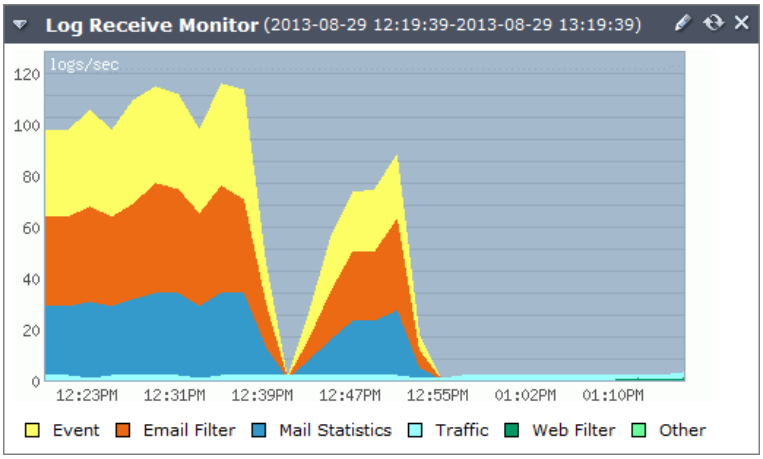
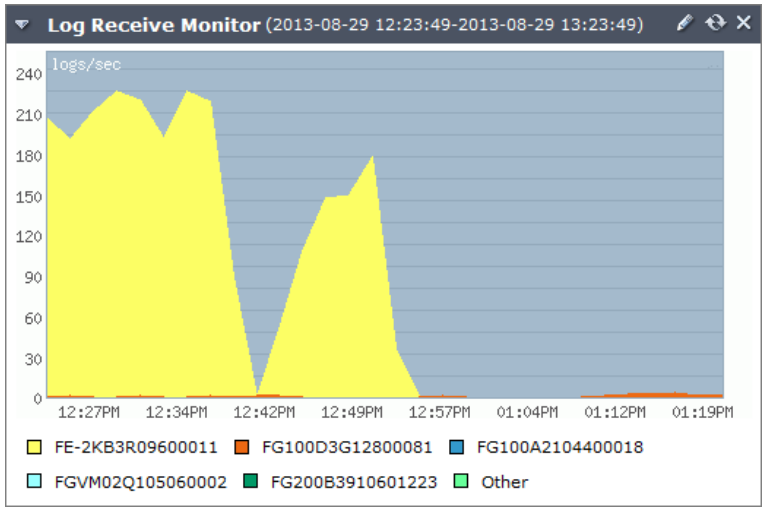
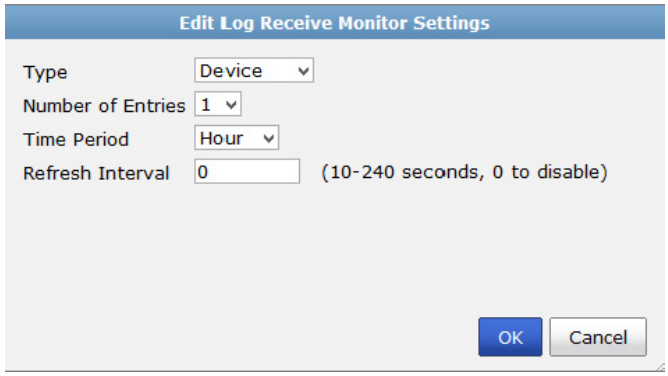


Figure 31: Log receive monitor widget (device)



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

Figure 32: Edit log receive monitor settings



Configure the following settings:

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

Logs/Data Received widget

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

Figure 33: Logs/data received widget (real-time)

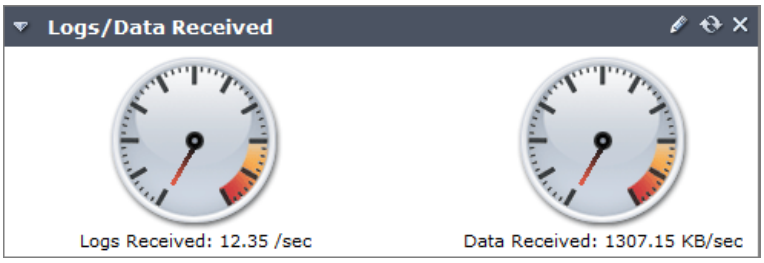
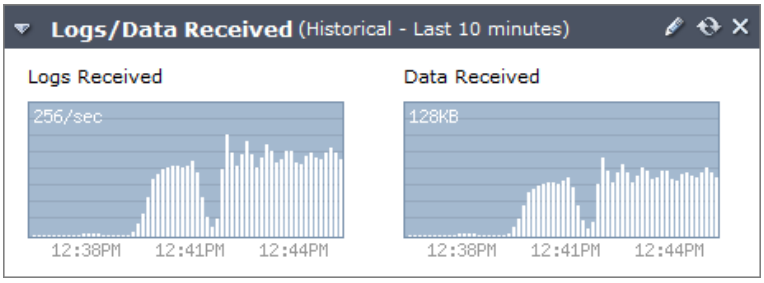


Figure 34: Logs/data received widget (historical)

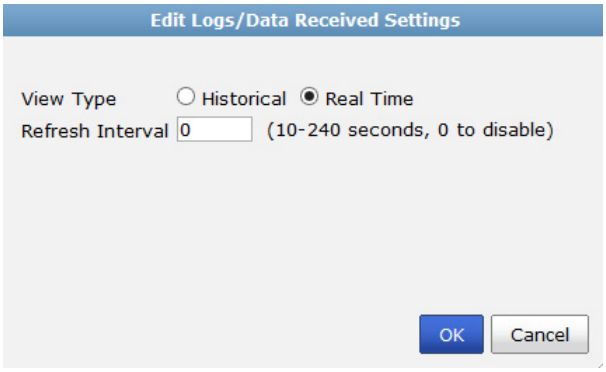


The widget displays the following information:

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

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

Figure 35: Edit logs/data received settings window



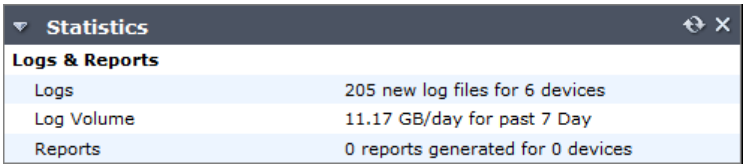
Configure the following settings:

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

Statistics widget

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

Figure 36: Statistics widget



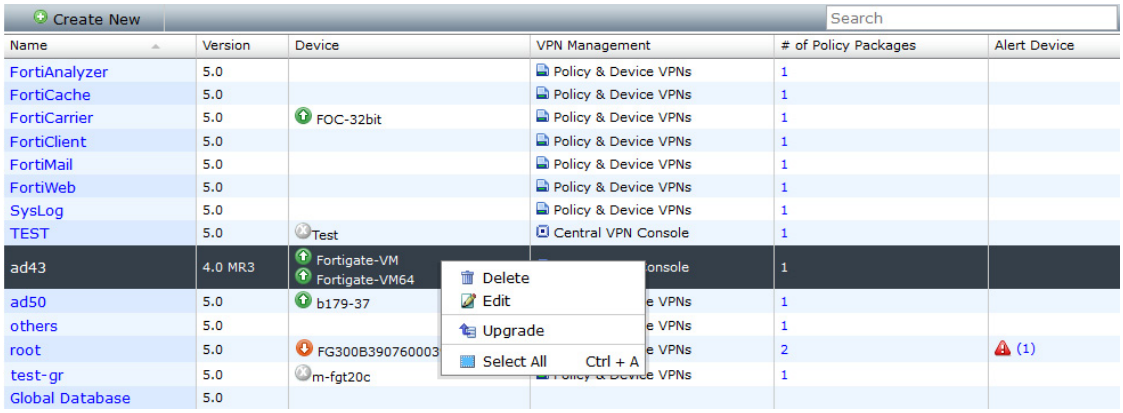
The widget displays the following information:

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

All ADOMs

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

Figure 37: All ADOMs



The following information is available:

Create New	Select to create a new ADOM. For information on creating a new ADOM, see “Adding an ADOM” on page 52
Name	The ADOM name.
Version	The ADOM version.
Device	The device or devices that the ADOM contains.
VPN Management	VPN management information for the ADOM.
# of Policy Packages	The number of policy packages currently used by the ADOM. Select the number to view a list of the policy packages and their installation targets.
Alert Device	The number of devices in the ADOM that currently have alerts. Select the number to view a list of the devices with alerts and the alert details.

The ADOMs in the list can also be edited and deleted as required. See “Managing ADOMs” on page 51 for more information.

The ADOM version can also be upgraded. See “Upgrading an ADOM” on page 54 for more information.



An ADOM can only be upgraded after all the devices within the ADOM have been upgraded. See “ADOM versions” on page 51 for more information.

RAID Management

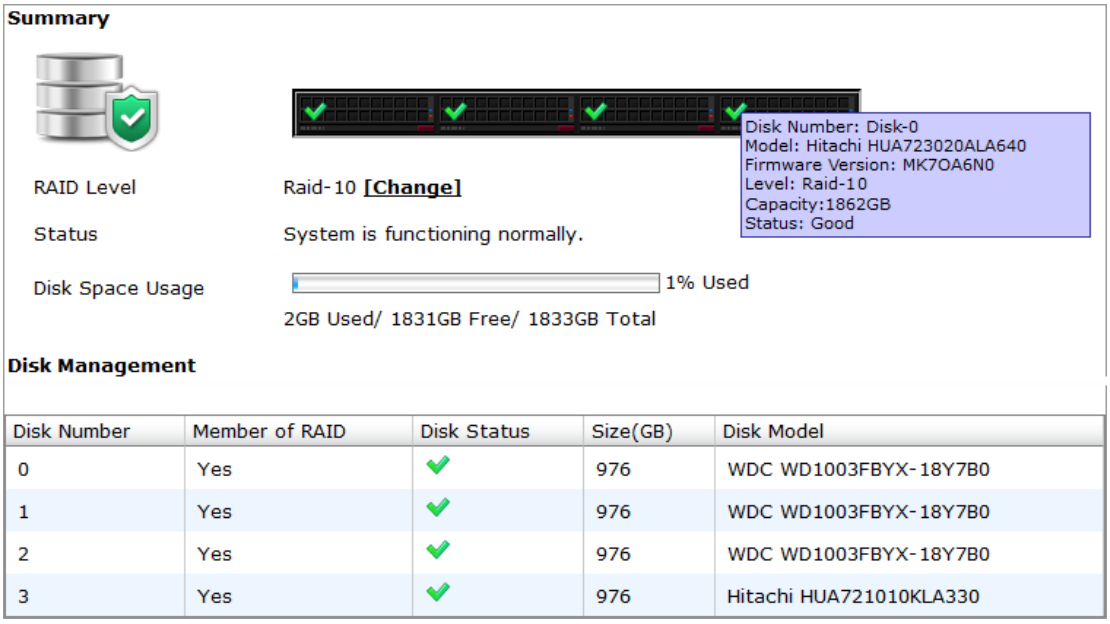
RAID helps to divide data storage over multiple disks, providing increased data reliability. FortiManager units that contain multiple hard disks can have RAID configured for capacity, performance, and availability.

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

The *Alert Message Console* widget, located in *System Settings* > *Dashboard*, provides detailed information about RAID array failures. For more information see “Alert Messages Console widget” on page 74.

If you need to remove a disk from the FortiManager unit, you may be able to hot swap it. Hot swapping means replacing a hard disk while the device is in operation. Hot swapping is a quick and efficient way to replace hard disks. For more information about hot swapping, see “Hot swapping hard disks” on page 84.

Figure 38:RAID Management page



The following information is displayed on this page:

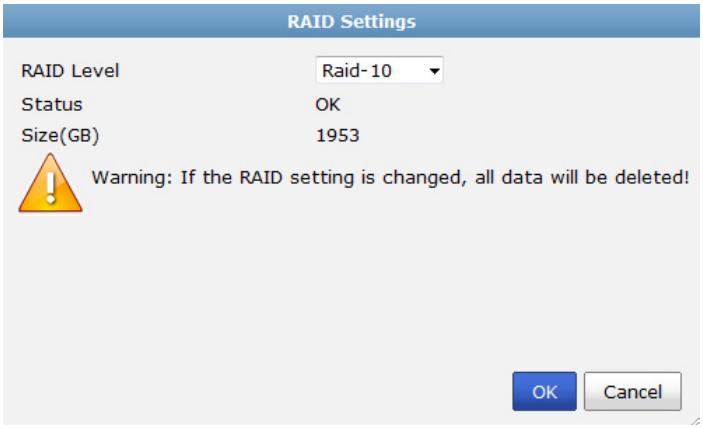
Summary	Hover the mouse cursor over a disk to view the disk number, model, firmware version, level, capacity, and status.
RAID Level	The RAID level. Select [Change] to change the RAID level. Select the RAID level from the drop-down list and select OK. *Note:* If RAID settings are changed, all data will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

To configure the RAID level:

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

   The *RAID Settings* dialog box opens.

Figure 39:RAID settings



3. From the *RAID Level* list, select the RAID option you want to use, then select *OK*.

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

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

Supported RAID levels

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

- ***Linear RAID***

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

- ***RAID 0***

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

- ***RAID 1***

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

- ***RAID 1 +Spare***

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

- ***RAID 5***

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

- ***RAID 5 +Spare***

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

- ***RAID 6***

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

- ***RAID 6 +Spare***

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

- ***RAID 10***

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

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

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

- ***RAID 50***

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

- ***RAID 60***

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

Hot swapping hard disks

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

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

To identify which hard disk failed, read the relevant log message in the *Alert Message Console* widget (see "Alert Messages Console widget" on page 74).

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



Electrostatic discharge (ESD) can damage FortiManager equipment. Only perform the procedures described in this document from an ESD workstation. If no such station is available, you can provide some ESD protection by wearing an anti-static wrist or ankle strap and attaching it to an ESD connector or to a metal part of a FortiManager chassis.
When replacing a hard disk, you need to first verify that the new disk has the same size as those supplied by Fortinet and has at least the same capacity as the old one in the FortiManager unit. Installing a smaller hard disk will affect the RAID setup and may cause data loss. Due to possible differences in sector layout between disks, the only way to guarantee that two disks have the same size is to use the same brand and model.
The size provided by the hard drive manufacturer for a given disk model is only an approximation. The exact size is determined by the number of sectors present on the disk.

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



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

Adding new disks

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



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

To add more hard disks:

1. Obtain the same disks as those supplied by Fortinet.
2. Back up the log data on the FortiManager unit.

   You can also migrate the data to another FortiManager unit if you have one. Data migration reduces system down time and risk of data loss. For information on data backup, see "Backing up the system" on page 66.

3. Install the disks on the FortiManager unit. If your unit supports hot swapping, you can do so while the unit is running.
4. Configure the RAID level.

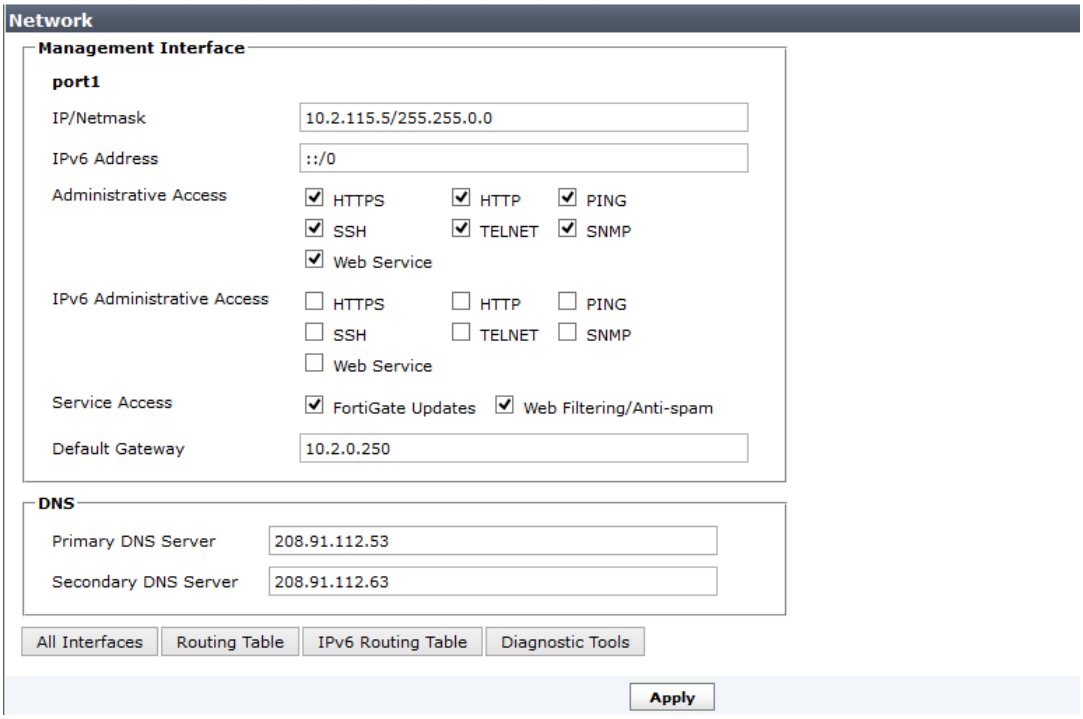
   If you have backed up the log data, restore the data. For more information, see "Restoring the configuration" on page 67.

Network

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

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

Figure 40: Network screen



The following information is available:

Management Interface	
IP/Netmask	The IP address and netmask associated with this interface.
IPv6 Address	The IPv6 address associated with this interface.
Administrative Access	Select the allowed administrative service protocols from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, and Web Service.
IPv6 Administrative Access	Select the allowed IPv6 administrative service protocols from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, and Web Service.

Service Access	Select the Fortinet services that are allowed access on this interface. These include FortiGate updates and web filtering /email filtering. By default all service access is enabled on port1, and disabled on port2.
Default Gateway	The default gateway associated with this interface
DNS	
Primary DNS Server	Enter the primary DNS server IP address.
Secondary DNS Server	Enter the secondary DNS server IP address.
All Interfaces	Click to open the network interface list. See "Viewing the network interface list" on page 86.
Routing Table	Click to open the routing table. See "Configuring static routes" on page 88.
IPv6 Routing Table	Click to open the IPv6 routing table. See "Configuring IPv6 static routes" on page 89.
Diagnostic Tools	Select to run available diagnostic tools, including *Ping*, *Traceroute*, and *View logs*.

Viewing the network interface list

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

Figure 41: Network interface list

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

The following information is available:

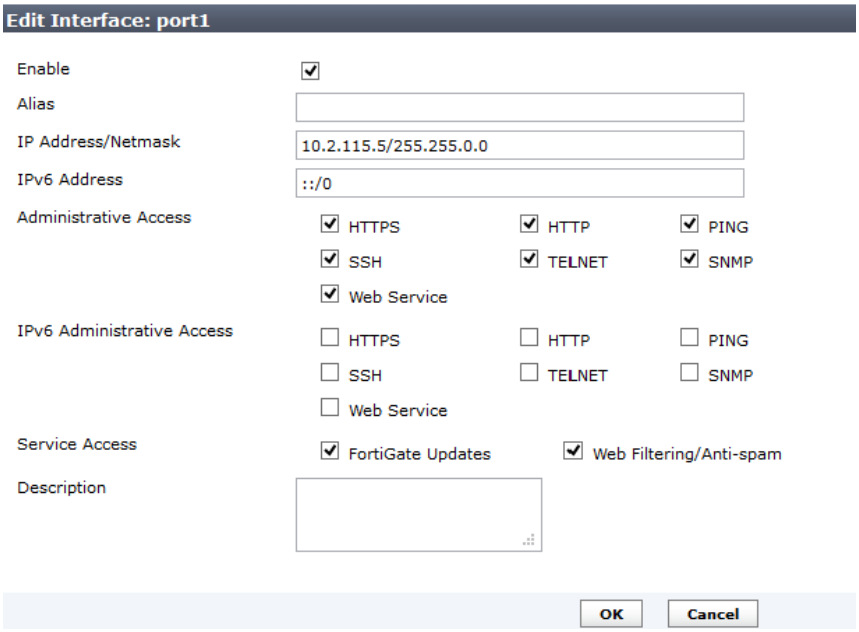
Name	The names of the physical interfaces on your FortiManager unit. The name, including number, of a physical interface depends on the model. Unlike FortiGate, you cannot set alias names for the interfaces. For more information, on configuring the interface, see "Configuring network interfaces" on page 87. If HA operation is enabled, the HA interface has */HA* appended to its name.
IP/Netmask	The IP address and netmask associated with this interface.
IPv6 Address	The IPv6 address associated with this interface.
Description	A description of the interface.

Administrative Access	The list of allowed administrative service protocols on this interface. These include HTTP, HTTPS, PING, SSH, and Telnet.
IPV6 Administrative access	The list of allowed IPv6 administrative service protocols on this interface.
Service Access	The list of Fortinet services that are allowed access on this interface. These include FortiGate updates, web filtering, and email filter. By default all service access is enabled on port1, and disabled on port2.
Enable	Displays if the interface is enabled or disabled. If the port is enabled, a green circle with a check mark appears in the column. If the interface is not enabled, a gray circle with an "X" appears in the column.

Configuring network interfaces

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

Figure 42: Configure network interfaces



The following settings are available.

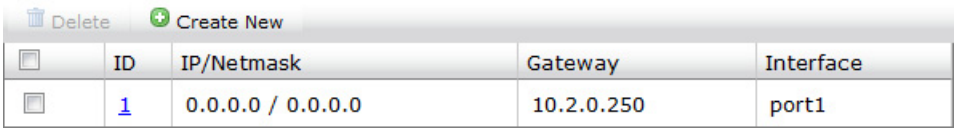
Enable	Select to enable this interface. A green circle with a check mark appears in the interface list to indicate the interface is accepting network traffic. When not selected, a gray circle with an "X" appears in the interface list to indicate the interface is down and not accepting network traffic.
Alias	Enter an alias for the port to make it easily recognizable.
IP Address/Netmask	Enter the IP address and netmask for the interface.
IPv6 Address	Enter the IPv6 address for the interface.

Administrative Access	Select the services to allow on this interface. Any interface that is used to provide administration access to the FortiManager unit will require at least HTTPS or HTTP for web-manager access, or SSH for CLI access.
IPv6 Administrative Access	Select the services to allow on this interface.
Service access	Select the services that will communicate with this interface.
Description	Enter a brief description of the interface (optional).

Configuring static routes

Go to *System Settings* > *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 43: Routing table



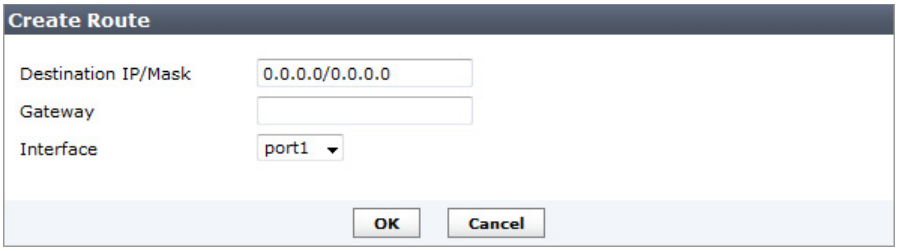
The following information is displayed:

Delete	Select the check box next to the route number and select *Delete* to remove the route from the table.
Create New	Select *Create New* to add a new route. See "Add a static route" on page 88. Select the route number to edit the settings.
ID	The route number.
IP/Netmask	The destination IP address and netmask for this route.
Gateway	The IP address of the next hop router to which this route directs traffic.
Interface	The network interface that connects to the gateway.

Add a static route

Go to *System Settings* > *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 44: Create new route



Configure the following settings:

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

Configuring IPv6 static routes

Go to *System Settings* > *Network* and select the *IPv6 Routing Table* button to view, edit, or add to the IPv6 static routing table. You may need to add entries to the routing table so that the FortiManager unit can reach FortiGate units on remote networks.

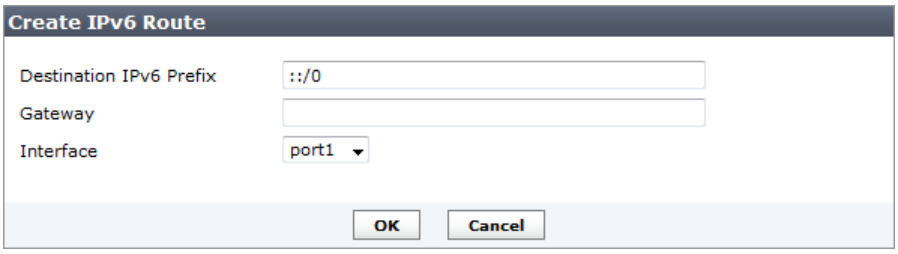
The following information and settings are available:

Delete	Select the check box next to the route number and select *Delete* to remove the route from the table.
Create New	Select *Create New* to add a new route. See "Add a IPv6 static route" on page 89. Select the route number to edit the settings.
ID	The route number.
IPv6 Address	The destination IPv6 address for this route.
Gateway	The IP address of the next hop router to which this route directs traffic.
Interface	The network interface that connects to the gateway.

Add a IPv6 static route

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

Figure 45: Create new IPv6 route



Configure the following settings:

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

Diagnostic tools

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

Figure 46: Diagnostic tools



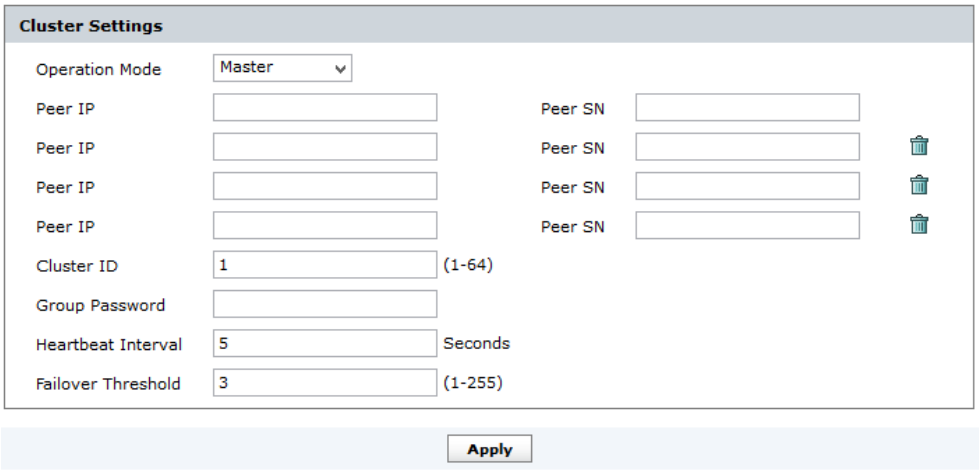
High Availability

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

Configuring HA options

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

Figure 47: Cluster settings dialog box



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.

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

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

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

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

For more information on High Availability, see "High Availability" on page 470.

Admin

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

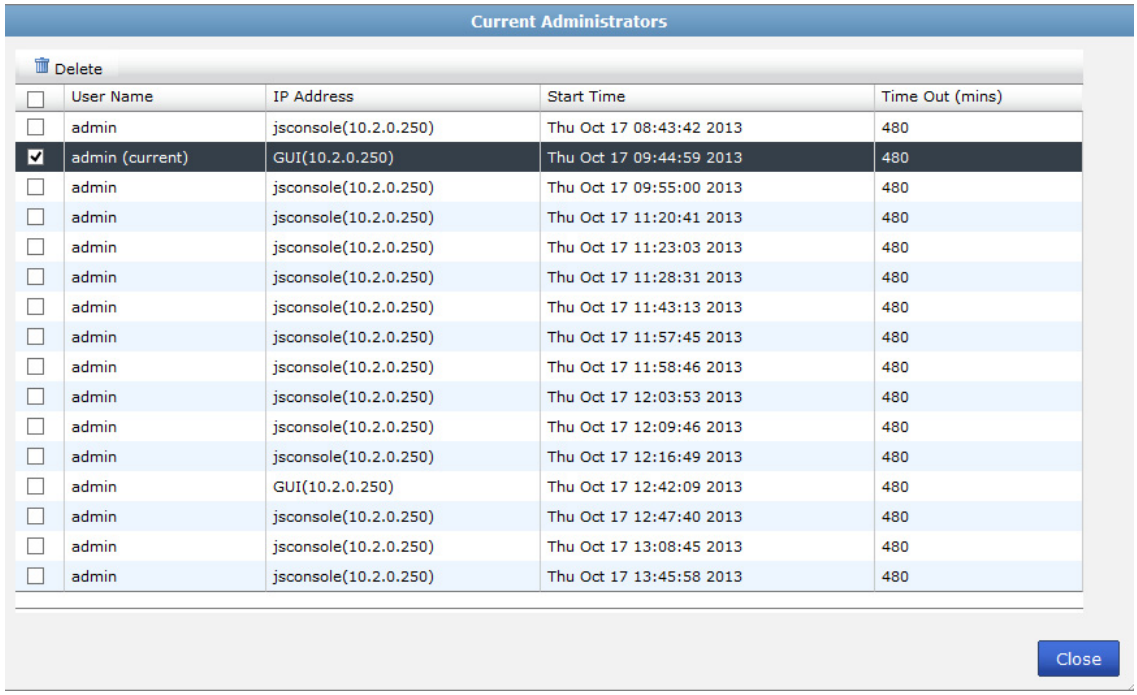
Administrator	Select to configure administrative users accounts. For more information, see "Administrator" on page 94.
Profile	Select to set up access profiles for the administrative users. For more information, see "Profile" on page 98.
Remote Auth Server	Select to configure authentication server settings for administrative log in. For more information, see "Remote authentication server" on page 101.
Admin Settings	Select to configure connection options for the administrator including port number, language of the Web-based Manager and idle timeout. For more information, see "Administrator settings" on page 105.

Monitoring administrator sessions

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

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

Figure 48: 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. This field also displays the login type (GUI, jsconsole, SSH, or telnet.
Start Time	The date and time the administrator logged in.
Time Out (mins)	The maximum duration of the session in minutes (1 to 480 minutes).
Delete	Select the check box next to the user and select *Delete* to drop their connection to the FortiManager unit.

To disconnect an administrator:

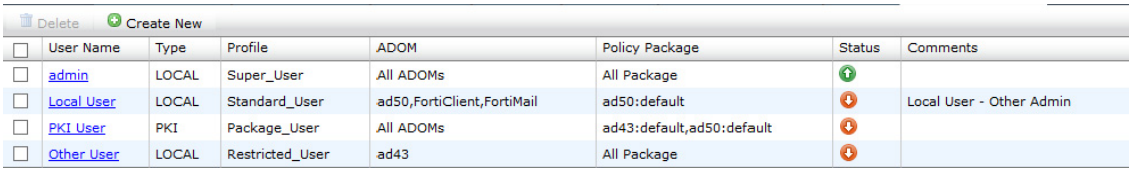
1. Go to *System Settings* > *Dashboard*.
2. In the System Information widget, under *Current Administrators*, select *[Detail]*. The list of current administrator sessions appears; see Figure 48.
3. Select the check box for each administrator session that you want to disconnect, and select *Delete*.
4. Select *OK* to confirm deletion of the session.

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

Administrator

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

Figure 49: Administrator list



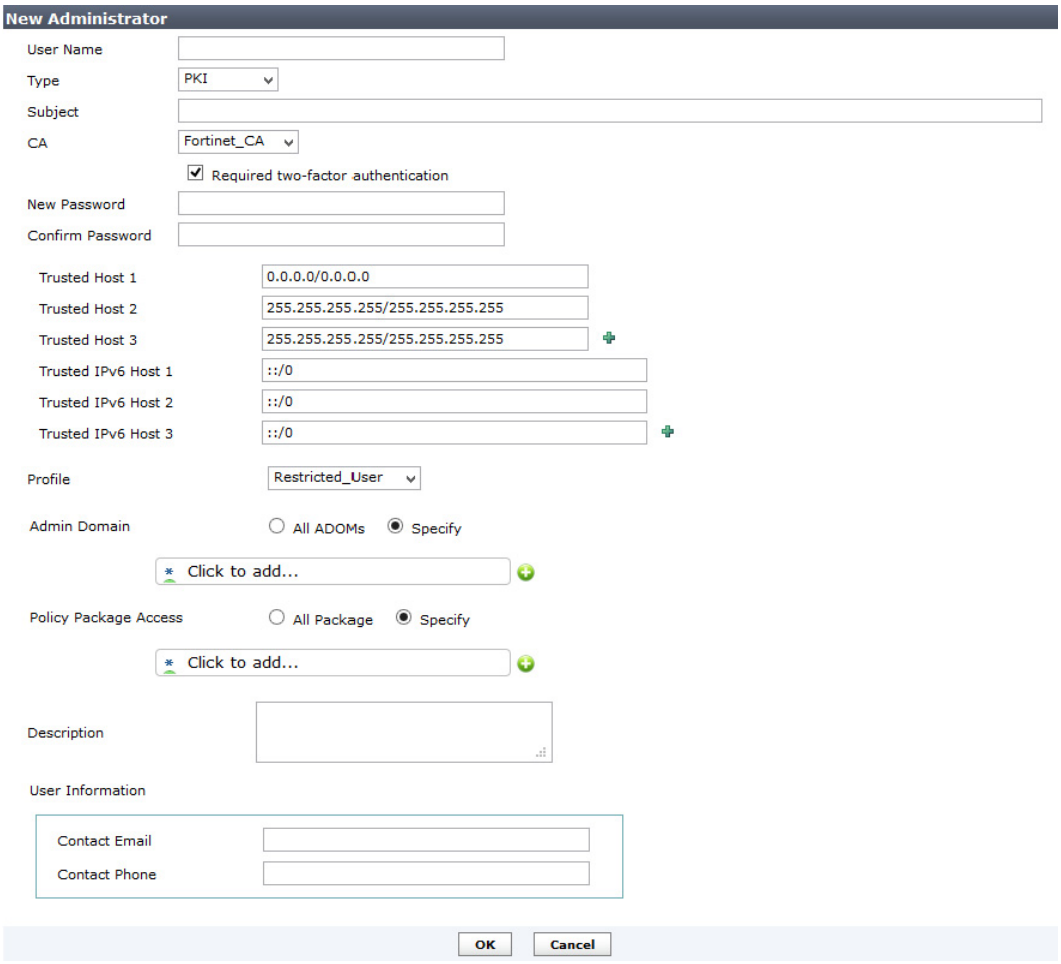
The following information is available:

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 95.
User Name	The name this administrator uses to log in. Select the administrator name to edit the administrator settings.
Profile	The administrator profile for this user that determines the privileges of this administrator. For information on administrator profiles, see "Profile" on page 98.
ADOM	The ADOM to which the administrator has been assigned.
Policy Package	The policy packages to which this profile allows access.
Status	Indicates whether the administrator is currently logged into the FortiManager unit not. A green circle with an up arrow indicates the administrator is logged in, a red circle with a down arrow indicates the administrator is not logged in.
Comments	Descriptive text about the administrator account.

To create a new administrator account:

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

Figure 50: 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. Select one of the following types: LOCAL, RADIUS, LDAP, TACACS+, or PKI.
RADIUS Server	Select the RADIUS server from the drop-down menu. *Note:* This field is available when the type is RADIUS.
LDAP Server	Select the LDAP server from the drop-down menu. *Note:* This field is available when the type is LDAP.

TACACS+ Server	Select the TACACS+ server from the drop-down menu. *Note:* This field is available when the type is TACACS+.
Wildcard	Select to enable wildcard. *Note:* This field is available when the type is RADIUS, LDAP, or TACACS+.
Subject	Enter a comment in the subject field for the PKI administrator. *Note:* This field is available when the type is PKI.
CA	Select the CA from the drop-down menu. *Note:* This field is available when the type is PKI.
Require two-factor authentication	Select to enable two-factor authentication. *Note:* This field is available when the type is PKI.
New Password	Enter the password. *Note:* This field is available if *Type* is *LOCAL, RADIUS, LDAP, TACACS+, or PKI*.
Confirm Password	Enter the password again to confirm it. *Note:* This field is available if *Type* is *LOCAL, RADIUS, LDAP, TACACS+, or PKI*.
Trusted Host1 **Trusted Host2** **Trusted Host3** **...** **TrustedHost10**	Optionally, enter the trusted host IP address and netmask from which the administrator can log in to the FortiManager unit. You can specify up to three trusted hosts. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see “Using trusted hosts” on page 97.
Trusted IPv6 Host1 **Trusted IPv6 Host2** **Trusted IPv6 Host3** **...** **TrustedIPv6 Host10**	Optionally, enter the trusted host IPv6 address from which the administrator can log in to the FortiManager unit. You can specify up to three trusted IPv6 hosts. Setting trusted IPv6 hosts for all of your administrators can enhance the security of your system. For more information, see “Using trusted hosts” on page 97.
Profile	Select a profile from the drop-down menu. The profile selected determines the administrator’s access to the FortiManager unit’s features. To create a new profile see “Configuring administrator profiles” on page 99.
Admin Domain	Choose the ADOMs this administrator will be able to access, or select *All ADOMs*. *Note:* This field is available only if ADOMs are enabled.
Policy Package Access	Choose the policy packages this administrator will have access to, or select *All Package*.

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.*
2. In the *User Name* column, double-click on the user name of the administrator you want to change. The *Edit Administrator* window appears.
3. Modify the settings as required. For more information about configuring account settings, see "To create a new administrator account:" on page 95.
4. Select *OK* to save your changes.

To delete an existing administrator account:

1. Go to *System Settings* > *Admin* > *Administrator.* The list of configured administrators appears; see Figure 49 on page 94.
2. Select the check box of the administrator account you want to delete and then select the *Delete* icon in the toolbar.
3. In the dialog box that appears, select *OK* to confirm the deletion.

Using trusted hosts

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

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

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



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

Profile

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

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

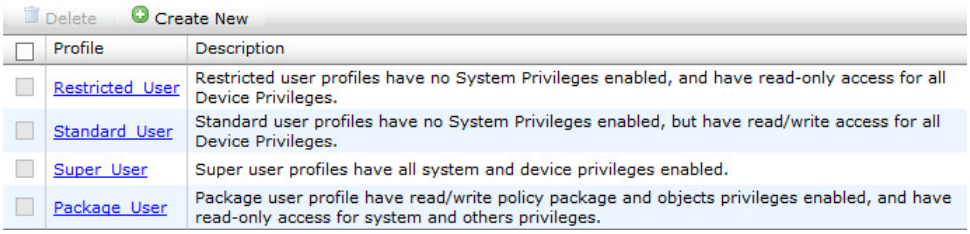
You cannot delete these profiles, but you can modify them. You can also create new profiles if required.



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

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

Figure 51: 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 99.

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 99.
Description	Provides a brief description of the system and device access privileges allowed for the selected profile.

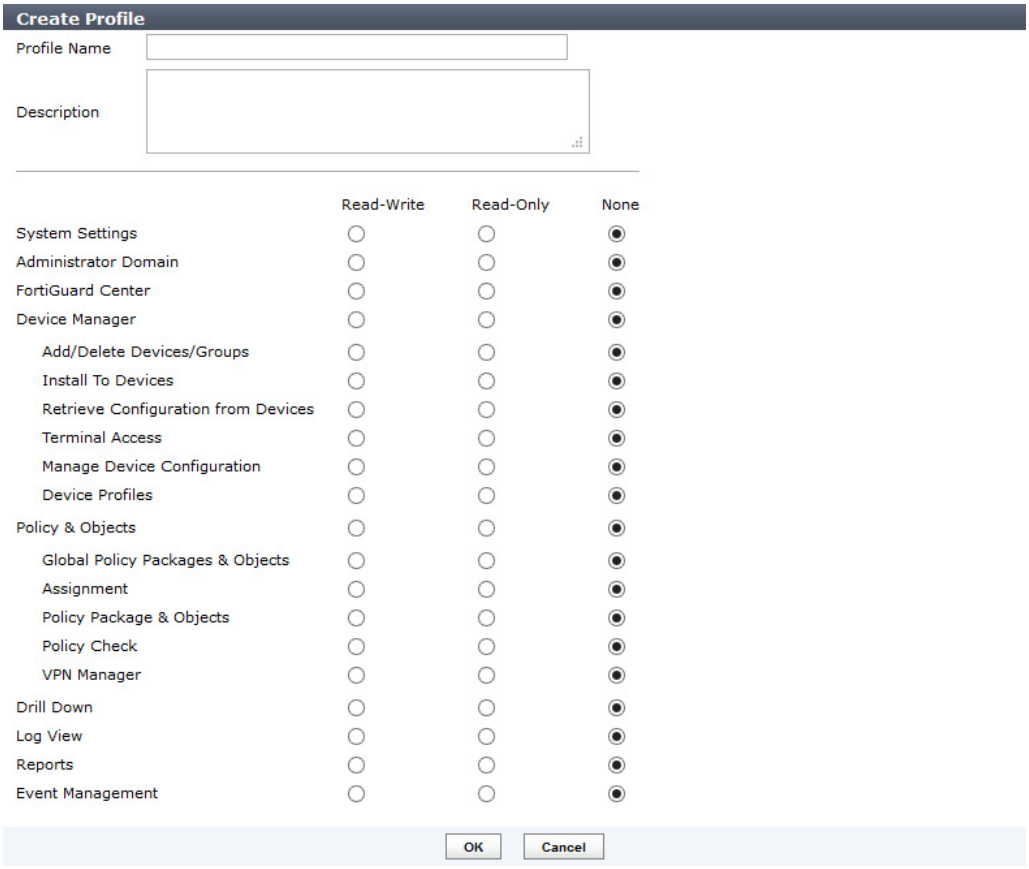
Configuring administrator profiles

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 52: Create new administrator profile



2. Configure the following settings:

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

Administrator Domain	Select *None*, *Read Only*, or *Read-Write* access.
FortiGuard Center	Select *None*, *Read Only*, or *Read-Write* access.
Device Manager	Select *None*, *Read Only*, or *Read-Write* access/
Add/Delete Devices/Groups	Select *None*, *Read Only*, or *Read-Write* access.
Install to Devices	Select *None*, *Read Only*, or *Read-Write* access.
Retrieve Configuration from Devices	Select *None*, *Read Only*, or *Read-Write* access.
Terminal Access	Select *None*, *Read Only*, or *Read-Write* access.
Manage Device Configuration	Select *None*, *Read Only*, or *Read-Write* access.
Device Profiles	Select *None*, *Read Only*, or *Read-Write* access.
Policy & Objects	Select *None*, *Read Only*, or *Read-Write* access.
Global Policy Packages & Objects	Select *None*, *Read Only*, or *Read-Write* access.
Assignment	Select *None*, *Read Only*, or *Read-Write* access.
Policy Packages & Objects	Select *None*, *Read Only*, or *Read-Write* access.
Policy Check	Select *None*, *Read Only*, or *Read-Write* access.
VPN Manager	Select *None*, *Read Only*, or *Read-Write* access.
Drill Down	Select *None*, *Read Only*, or *Read-Write* access.
Log View	Select *None*, *Read Only*, or *Read-Write* access.
Reports	Select *None*, *Read Only*, or *Read-Write* access.
Event Management	Select *None*, *Read Only*, or *Read-Write* access.

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

To modify an existing profile:

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

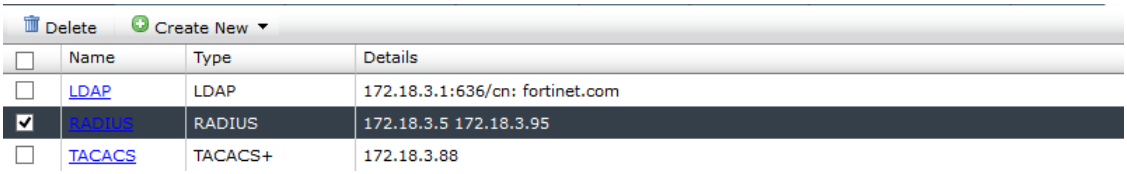
To delete a profile:

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

Remote authentication server

The FortiManager system supports remote authentication of administrators using LDAP, RADIUS, and TACACS+ servers. To use this feature, you must configure the appropriate server entries in the FortiManager unit for each authentication server in your network. New remote authentication servers can be added. Existing servers can be modified and deleted as required; see “Manage remote authentication servers” on page 104.

Figure 53: Remote authentication server list



The following options are available:

Delete	Delete the selected server.
Create New	Create a new server. Select one of LDAP, RADIUS, or TACACS+ from the drop-down list.
Name	The name of the server.
Type	The server type. One of LDAP, RADIUS, or TACACS+.
Details	Details about the server, such as the IP address.

LDAP

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

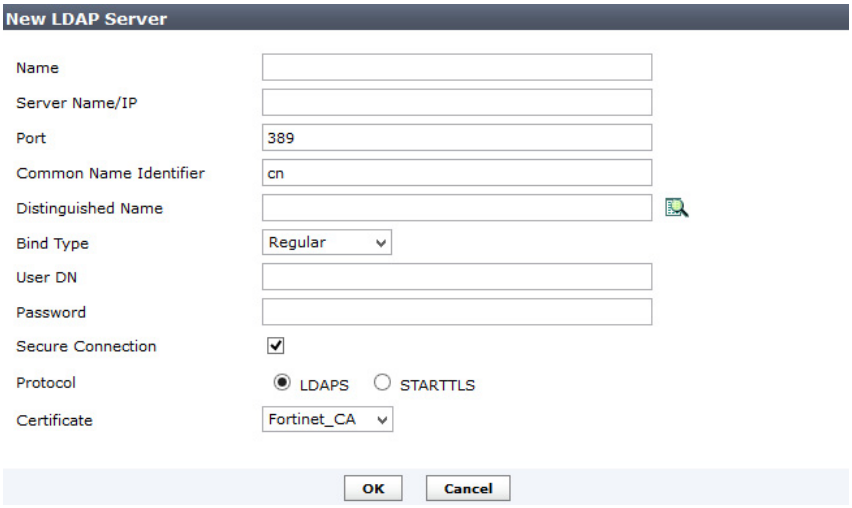
If you have configured LDAP support and require a user to authenticate using an LDAP server, the FortiManager unit contacts the LDAP server for authentication. To authenticate with the FortiManager unit, the user enters a user name and password. The FortiManager unit sends this user name and password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

To add an LDAP server:

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

   The *New LDAP Server* window opens.

Figure 54: 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	The distinguished name used to look up entries on the LDAP servers use. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. Selecting the *query distinguished name* button will query the LDAP for the name and open the *LDAP Distinguished Name Query* window to display the results.
Bind Type	Select the type of binding for LDAP authentication. Select Simple, Anonymous or Regular from the drop-down menu.,
User DN	When the *Bind Type* is set to *Regular*, enter the user DN.
Password	When the *Bind Type* is set to *Regular*, enter the password.
Secure Connection	Select to use a secure LDAP server connection for authentication.
Protocol	When *Secure Connection* is enabled, select either LDAPS or STARTTLS.
Certificate	When *Secure Connection* is enabled, select the certificate from the drop-down menu.

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

RADIUS

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

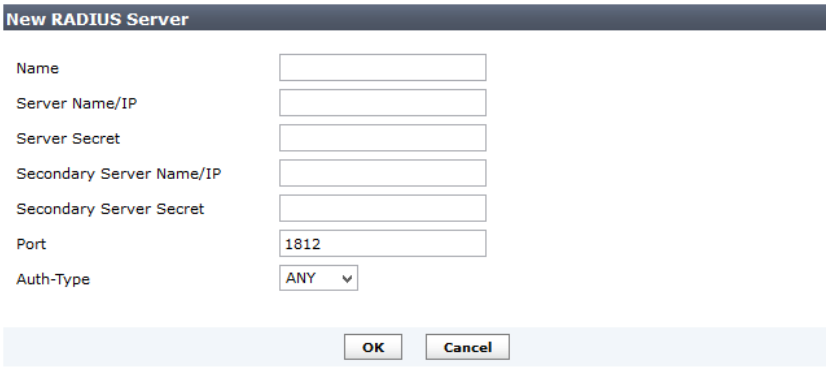
You can create or edit RADIUS server entries in the server list to support authentication of administrators. When an administrator account's type is set to RADIUS, the FortiManager unit uses the RADIUS server to verify the administrator password at logon. The password is not stored on the FortiManager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

To add a RADIUS server:

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

   The *New RADIUS Server* window opens.

Figure 55: 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. Select one of: ANY, PAP, CHAP, or MSv2.

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

TACACS+

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

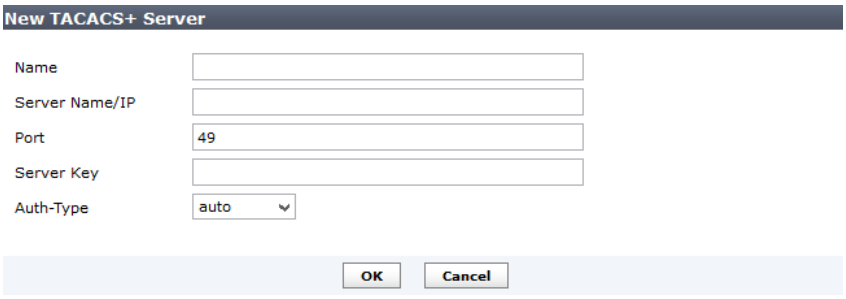
For more information about TACACS servers, see the FortiGate documentation.

To add a TACACS+ server:

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

   The *New TACACS+ Server* window opens.

Figure 56: 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 *auto* has the FortiManager unit try all the authentication types. Select one of: auto, ASCII, PAP, CHAP, or MSCHAP.

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

Manage remote authentication servers

Remote authentication servers can be modified and deleted as required.

To modify an existing server configuration:

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

To delete an existing server configuration:

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



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

Administrator settings

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

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

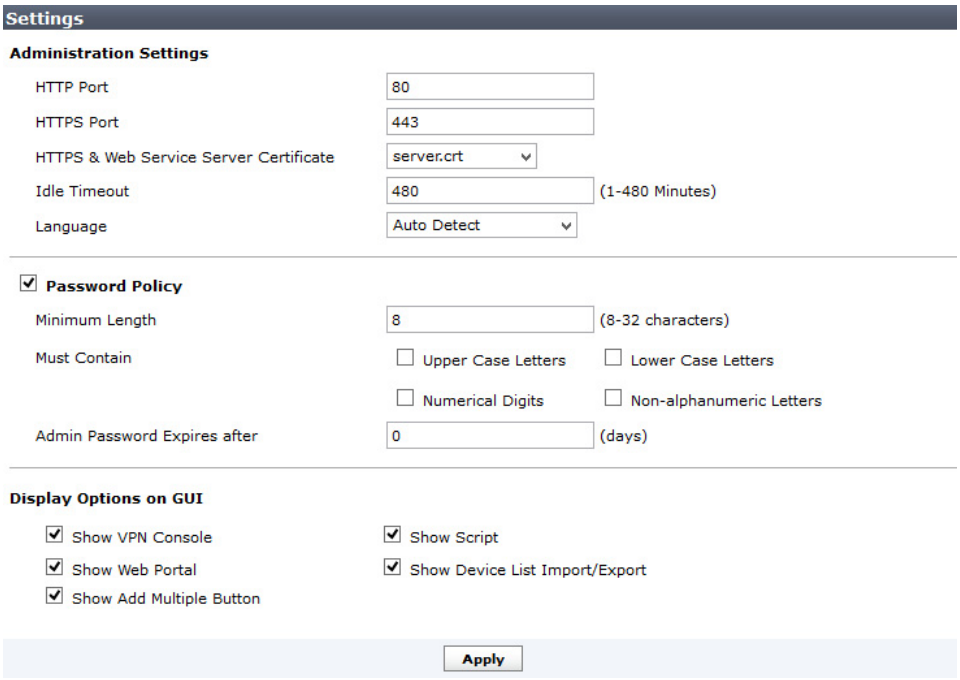
Only the `admin` administrator can configure these system options, which apply to all administrators logging onto the FortiManager unit.

To configure the administrative settings:

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

   The *Settings* window opens.

Figure 57: Administrative settings dialog box



2. Configure the following information:

Administration Settings	
HTTP Port	Enter the TCP port to be used for administrative HTTP access.
HTTPS Port	Enter the TCP port to be used for administrative HTTPS access.
HTTPS & Web Service Server Certificate	Select a certificate from the drop-down list.
Idle Timeout	Enter the number of minutes that an administrative connection can be idle before the administrator must log in again. The maximum is 480 minutes (8 hours). To ensure security, the idle timeout should be a short period of time to avoid the administrator inadvertently leaving the management computer logged in to the FortiManager unit and opening the possibility of someone walking up and modifying the network options.
Language	Select a language from the drop-down list.
Password Policy	Select to enable administrator passwords.
Minimum Length	Select the minimum length for a password. The default is eight characters.
Must Contain	Select the types of characters that a password must contain.
Admin Password Expires after	Select the number of days that a password is valid for, after which time it must be changed.
Display Option on GUI	
Display Options on GUI	Select the required options from the list.
Show VPN Console	Select to display the VPN Console menu item. This menu is located in the *Policy & Objects* tab under Policy Package in the left-hand tree menu. VPN Console is available when ADOM *VPN Management* is set to *Central VPN Console*. This is an advanced FortiManager feature.
Show Script	Select to display the *Script* menu item. This menu is located in the *Device Manager* tab under *Devices & Groups* in the left-hand tree menu. This is an advanced FortiManager feature.
Show Web Portal	Select to display the *Web Portal* menu item. This menu is located in the *Device Manager* tab under *Devices & Groups* in the left-hand tree menu. This is an advanced FortiManager feature.

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

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

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.

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

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

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

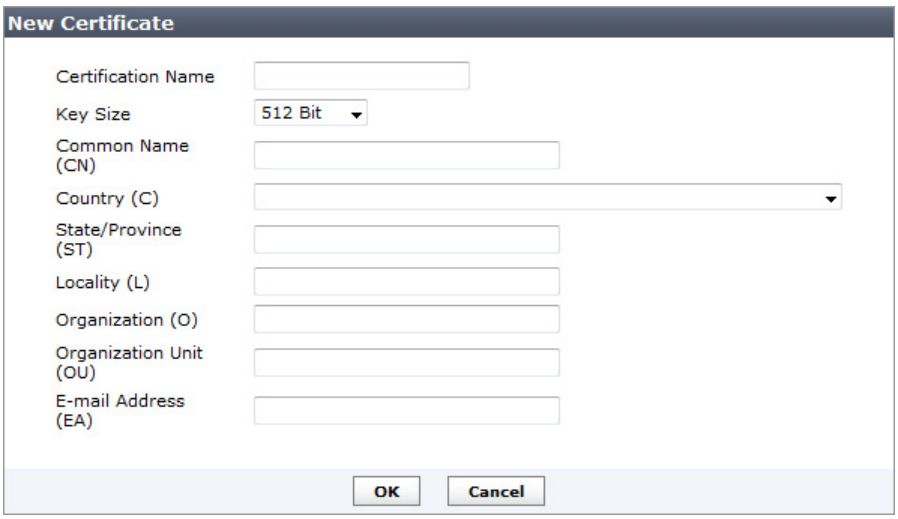
Creating a local certificate

To create a certificate request:

1. Go to *System Settings* > *Certificates* > *Local Certificates*.
2. Select the *Create New* button.

   The *New Certificate* window opens.

Figure 58: New local certificate



3. Enter the following information as required.

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

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

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



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

Importing certificates

To import a local certificate:

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

To import a CA certificate:

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

Importing CRLs

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

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

To import a CRL:

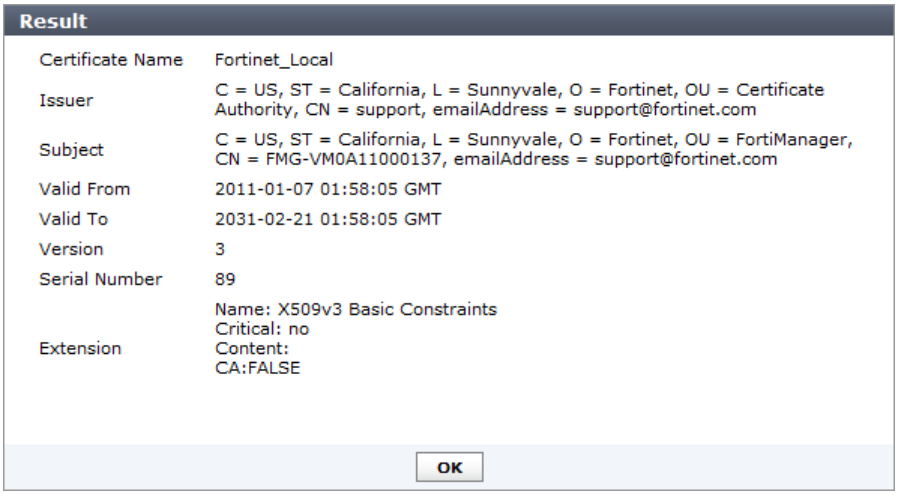
1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the *Import* button.
3. Enter the location of the certificate, or select *browse* and browse to the location of the certificate, then select *Ok*.

Viewing certificate details

To view a local certificate:

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

Figure 59: Local certificate detail



The following information is displayed:

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

3. Select *OK* to continue.

To view a CA certificate:

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

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

To view a CRL:

1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the certificates which you would like to see details about and click on *View Certificate Detail*.
3. The details displayed are similar to those displayed for a local certificate.

Downloading a certificate

To download a local certificate:

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

To download a CA certificate:

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

Event Log

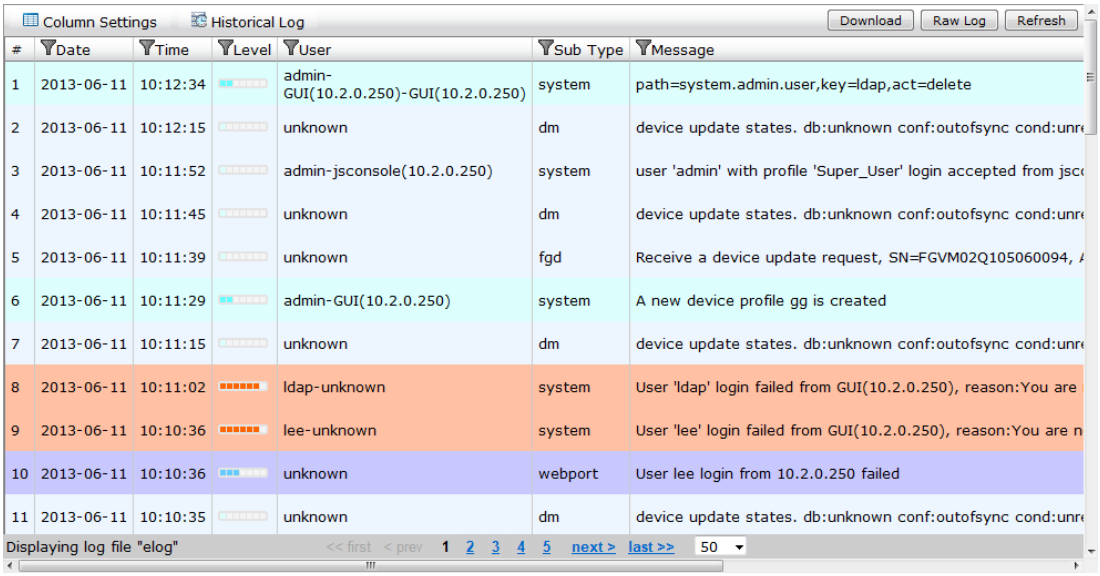
The logs created by FortiManager are viewable within the Web-based Manager. You can use the *FortiManager Log Message Reference*, available on the Fortinet Technical Documentation web site to interpret the messages. You can view log messages in the FortiManager Web-based Manager that are stored in memory or on the internal hard disk.

To view the log messages:

1. Go to *System Settings* > *Event Log*.

   The event log window opens.

Figure 60: Event log table



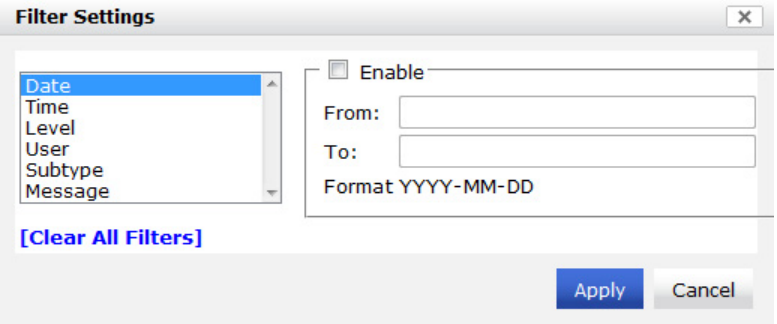
The following information is displayed:

Column Settings	Select *Column Settings* to open the *Column Settings* window and adjust the column settings for the list.
Historical Log	Select *Historical Log* to view historical event logs. You can view select Event Log, FDS Upload Log, or FDS Download Log from the drop-down menu. You can select to clear or view logs. The following columns are displayed: File Name, Size, and Last Access Time.

Download	Select *Download* to download a file containing the logs in either CSV or the normal format. Select *OK* to save the file to your management computer.
Raw Log	Select the *Raw Log*/*Formatted Table* button to toggle log message view. Raw logs are displayed in the following format: `2013-10-17 14:26:01 log_id=0001013001 type=event subtype=fgfm pri=warning adom=n/a user=fgfm msg="fgfm connection to device FG300B3907600039 is down"`
Refresh	Select *Refresh* to refresh the displayed logs.
#	The event log entry identifier.
Date	The date that the log was generated. You can select the filter icon to select a specific date range to view specific log entries. Select *[Clear All Filters]* to clear all filters that have been configured. Format: YYYY-MM-DD
Time	The time that the log was generated. You can select the filter icon to select a specific time range to view specific log entries. Select *[Clear All Filters]* to clear all filters that have been configured. Format: HH:MM:SS
Level	The logging level of the log generated. You can select the filter icon to select a logging level or range to view specific log entries. Select *[Clear All Filters]* to clear all filters that have been configured. The logging levels are Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug.
User	The user associated with the log generated. You can select the filter icon to enable specific event types. Select *[Clear All Filters]* to clear all filters that have been configured.
Sub Type	The logging subtype of the log generated. You can select the filter icon to select a logging level or range to view specific log entries. Select *[Clear All Filters]* to clear all filters that have been configured. The logging subtypes are System manager event, FG-FM protocol event, Device configuration event, Global database event, Script manager event, Web portal event, Firewall objects event, Policy console event, VPN console event, Endpoint manager event, Revision history event, Deployment manager event, HA event, Firmware manager event, FortiGuard service event, FortiClient manager event, FortiMail manager event, Debug I/O log event, Configuration change event, Device manager event, and Web service event.
Message	The log event message.
<< first ,< prev 1 2 3 4 5 next > last >> 50	Browse pages in the event log page. You can select the number of log entries to display from the drop-down menu.

2. Select the filter symbol in the heading of any of the table columns to open the *Filter Settings* window.

Figure 61: Filter settings window



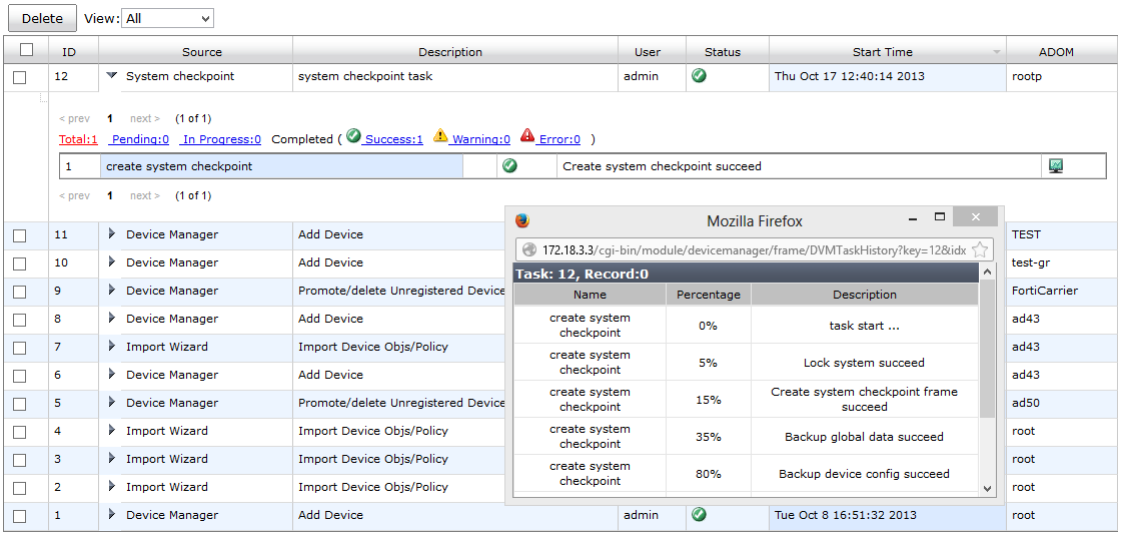
3. Adjust the filter settings as needed, then select *Apply* to apply the filter to the table.
4. Select *Clear Filter* from the event log table view to remove any applied filters.

Task Monitor

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

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

Figure 62: Task monitor window



The following information is displayed:

Delete	Remove the selected task or tasks from the list.
View	Select which tasks to view from the drop-down list, based on their status. The available options are: *Running*, *Pending*, *Done*, *Error*, *Cancelling*, *Cancelled*, *Aborting*, *Aborted*, *Warning*, and *All* (default).
ID	The identification number for a task.
Source	The platform from where the task is performed.

Expand Arrow	Select to display the specific actions taken under this task. To filter the specific actions taken for a task, select one of the options on top of the action list. Select the history icon to view specific information on task progress. This can be useful when troubleshooting warnings and errors.
Description	The nature of the task.
User	The users who have performed the tasks.
Status	The status of the task (hover over the icon to view the description): • *All*: All types of tasks. • *Done*: Completed with success. • *Error*: Completed without success. • *Cancelled*: User cancelled the task. • *Cancelling*: User is cancelling the task. • *Aborted*: The FortiManager system stopped performing this task. • *Aborting*: The FortiManager system is stopping performing this task. • *Running*: Being processed. In this status, a percentage bar appears in the Status column.
Start Time	The time that the task was performed.
ADOM	The ADOM to which the task applies.

Advanced

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

SNMP v1/v2c	Select to configure FortiGate and FortiManager reporting through SNMP traps. See “SNMP v1/v2c” on page 115.
Mail Server	Select to configure mail server settings for alerts, edit existing settings, or delete mail servers. See “Mail Server” on page 121.
Syslog Server	Select to configure syslog server settings for alerts, edit existing settings, or delete syslog servers.See “Syslog Server” on page 122.
Meta Fields	Select to configure metadata fields for FortiGate objects, and for FortiGate-5000 series shelf managers. See “Meta Fields” on page 123
Device Log Settings	Select to configure log settings and access. See “Device Log Settings” on page 125
Advanced Settings	Select to configure global advanced settings such as offline mode, device synchronization settings and install interface policy only; see “Advanced Settings” on page 127.

SNMP v1/v2c

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

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

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

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

The FortiManager SNMP implementation is read-only — SNMP v1 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.

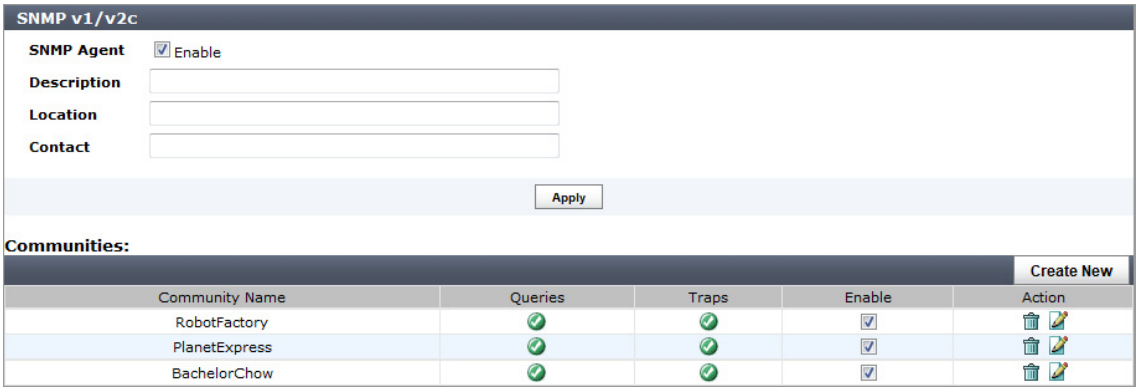
Configuring the SNMP agent

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

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

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

Figure 63:SNMP configuration



The following information is 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.
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 116.
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 deselect 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.



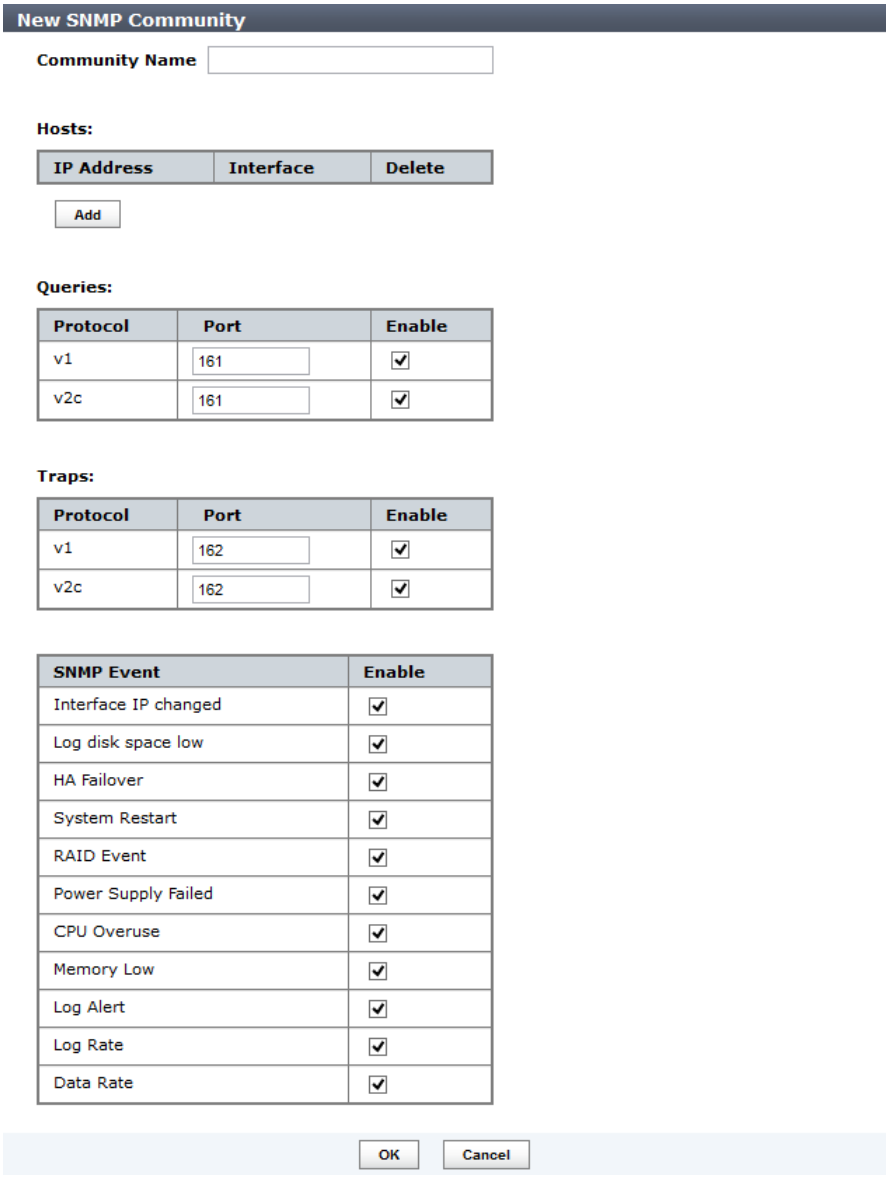
These SNMP communities do not refer to the FortiGate devices the FortiManager system is managing.

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

Select *Create New* on the SNMP v1/v2c screen to open the *New SNMP Community* dialog box, where you can configure a new SNMP community. See Figure 64 on page 117.

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 64: 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 from the drop-down list. You need to do this if the SNMP manager is on the Internet or behind a router.
Delete icon	Select to remove this SNMP manager entry.

Add	Select to add a new default entry to the Hosts list that you can edit as needed. You can have up to eight SNMP manager entries for a single community.
Queries	Enter the port numbers (161 by default) that the FortiManager system uses to send SNMP v1 and SNMP v2c queries to the FortiManager in this community. Enable queries for each SNMP version that the FortiManager system uses.
Traps	Enter the Remote port numbers (162 by default) that the FortiManager system uses to send SNMP v1 and SNMP v2c traps to the FortiManager in this community. Enable traps for each SNMP version that the FortiManager system uses.
SNMP Event	Enable the events that will cause the FortiManager unit to send SNMP traps to the community. These events include: *Interface IP changed*, *Log disk space low*, *HA Failover*, *System Restart*, *RAID Event*, *Power Supply Failed*, *CPU Overusage*, *Memory Low*, *Log Alert*, *Log Rate*, and *Data Rate*.

Fortinet MIBs

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

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

The Fortinet and FortiManager MIBs are listed in Table 2 along with the two RFC MIBs. You can obtain these MIB files from Customer Service & Support. To be able to communicate with the SNMP agent, you must compile all of these MIBs into your SNMP manager. Generally your SNMP manager will be an application on your local computer.

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

Table 2: Fortinet MIBs

MIB file name or RFC	Description
FORTINET-CORE-MIB.mib	The proprietary Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor Fortinet unit configuration settings and receive traps from the Fortinet SNMP agent. For more information, see “Fortinet traps” on page 119 and “Fortinet & FortiManager MIB fields” on page 120.
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 120.

Table 2: Fortinet MIBs (continued)

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

Fortinet traps

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

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

Table 3: Generic Fortinet traps

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

Table 4: Fortinet system traps

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

Table 4: Fortinet system traps (continued)

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

Table 5: FortiManager HA traps

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

Fortinet & FortiManager MIB fields

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

Table 6: System MIB fields

MIB field	Description
fnSysSerial	Fortinet unit serial number.

Table 7: Administrator accounts

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

Table 8: Custom messages

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

Table 9: FortiManager MIB fields and traps

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

Mail Server

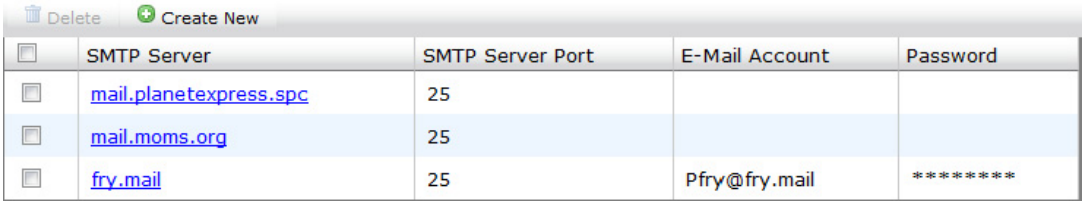
Configure mail server settings for alerts, edit existing settings, or delete mail servers.



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

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

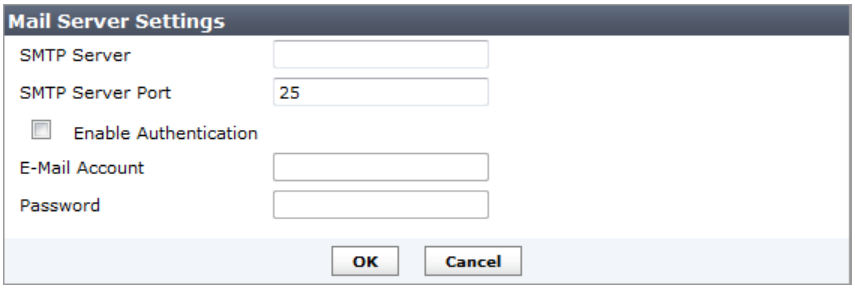
Figure 65: Mail server window



To create a new mail server:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Select *Create New*.
   The *Mail Server Settings* window opens.

   Figure 66: Mail server settings



3. Configure the following settings:

SMTP Server	Enter the SMTP server domain information, e.g. mail@company.com.
SMTP Server Port	Enter the SMTP server port number.
Enable Authentication	Select to enable authentication.

Email Account	Enter an email account, e.g. admin@company.com.
Password	Enter the email account password.

4. Select *OK* to save the setting.

To edit a mail server:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Select the *Edit* icon on the far right side of the server's row that you would like to edit.
   The *Mail Server Settings* window opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

To delete a mail server:

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

Syslog Server

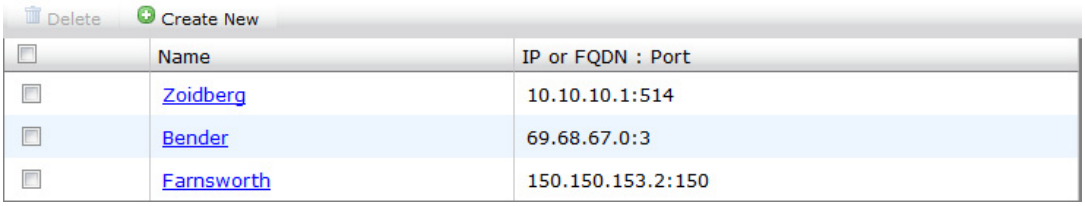
Configure syslog server settings for alerts, edit existing settings, or delete syslog servers.



If an existing syslog server is used in an event handler, the delete icon is removed and the syslog server entry can not be deleted.

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

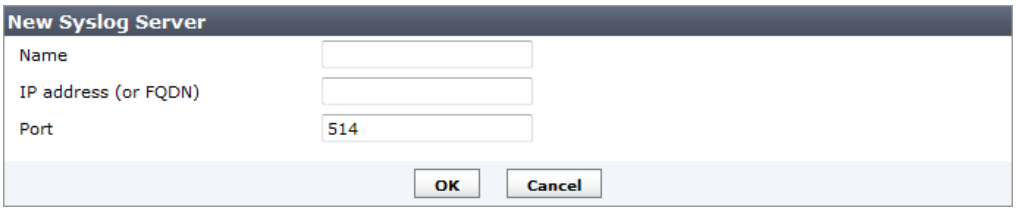
Figure 67: Syslog server window



To create a new syslog server:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Select *Create New*.
   The *New Syslog Server* window opens.

Figure 68: Syslog server settings



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

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

To edit a syslog server:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Select the *Edit* icon on the far right side of the server's row that you would like to edit.
   The *Edit Syslog Server* window opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

To delete a syslog server:

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

Meta Fields

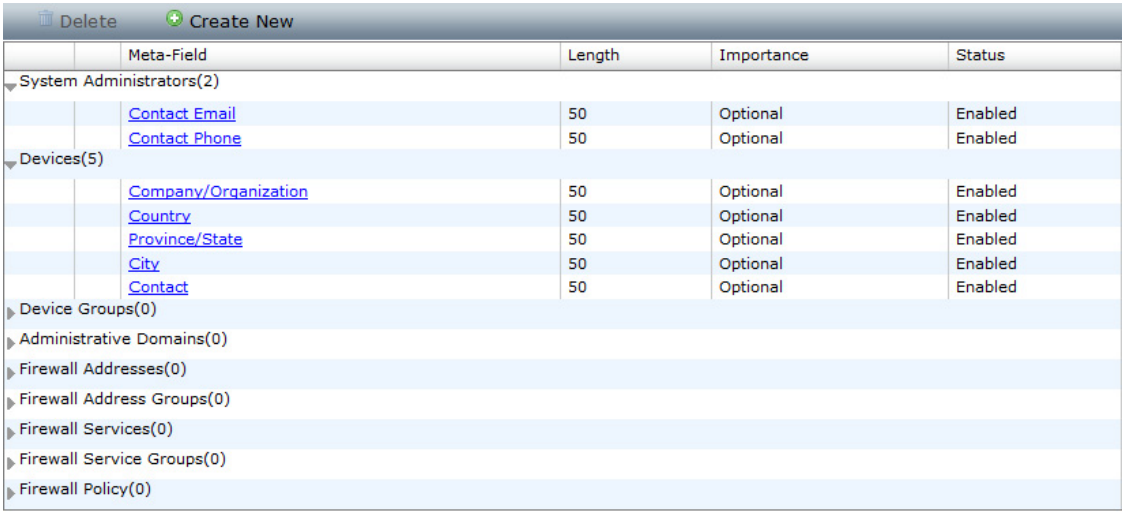
The *System Settings* > *Advanced* > *Meta Fields* menu enables you and other administrators to add extra information when configuring, adding, or maintaining FortiGate units or adding new administrators. You can make the fields mandatory or optional, and set the side of the field.

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.

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

Figure 69: Metadata



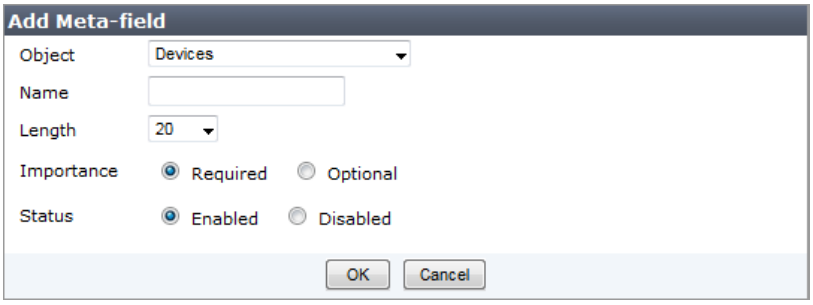
The following information is available:

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

To add a new metadata field:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
   The list of configured meta data objects appears; see Figure 69.
2. Select *Create New*.
   The *Add Meta-field* dialog box opens.

Figure 70: Add a meta field



3. Configure the following settings:

Object	The object to which this metadata field applies. Select one of the following: System Administrators, Devices, Device Groups, Administrative Domains, Firewall Addresses, Firewall Address Groups, Firewall Services, Firewall Service Groups, and Firewall Policy.
Name	Enter the label to use for the field.
Length	Select the maximum number of characters allowed for the field from the drop-down list (20, 50, or 255).
Importance	Select *Required* to make the field compulsory, otherwise select *Optional.*
Status	Select *Disabled* to disable this field. This field is only available for non-firewall objects. The default setting is *Enabled*.

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

To edit a metadata field:

1. Go to *System Settings* > *Advanced* > *Meta Fields.*
2. Select the name of the meta field that you would like to edit to open the *Edit Meta-field* dialog box.

   Only the length, importance, and status of the meta field can be edited.
3. Edit the settings as required, and then select *OK* to apply the changes.

To delete metadata fields:

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

   The default meta fields cannot be deleted.
3. Select the *Delete* icon in the toolbar, then select *OK* in the confirmation box to delete the fields.

Device Log Settings

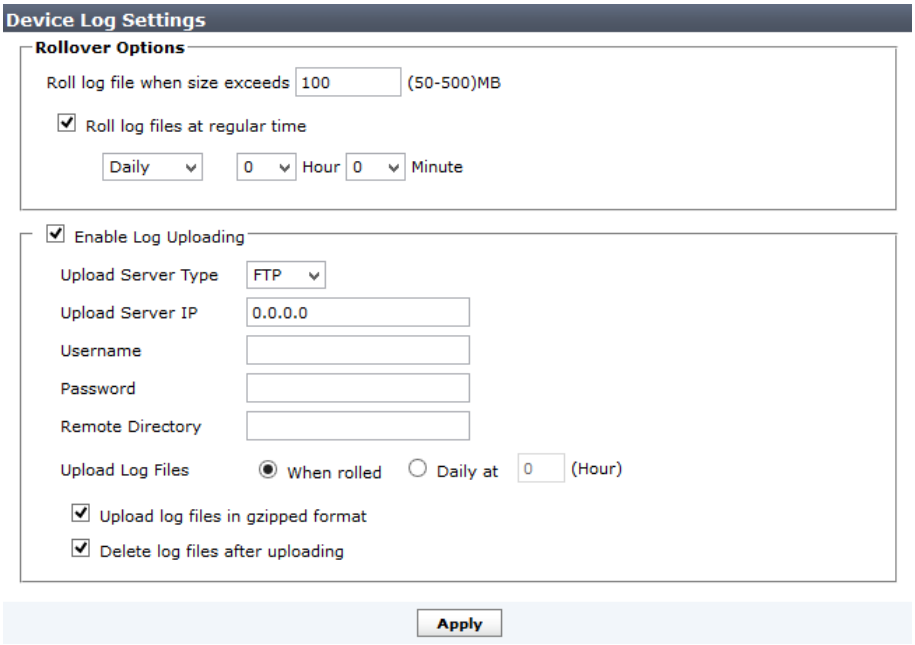
The FortiManager allows you to log system events to disk. For more information, see "Log View" on page 359.

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

- Log rotation settings
- Log uploading

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

Figure 71: Device log setting window



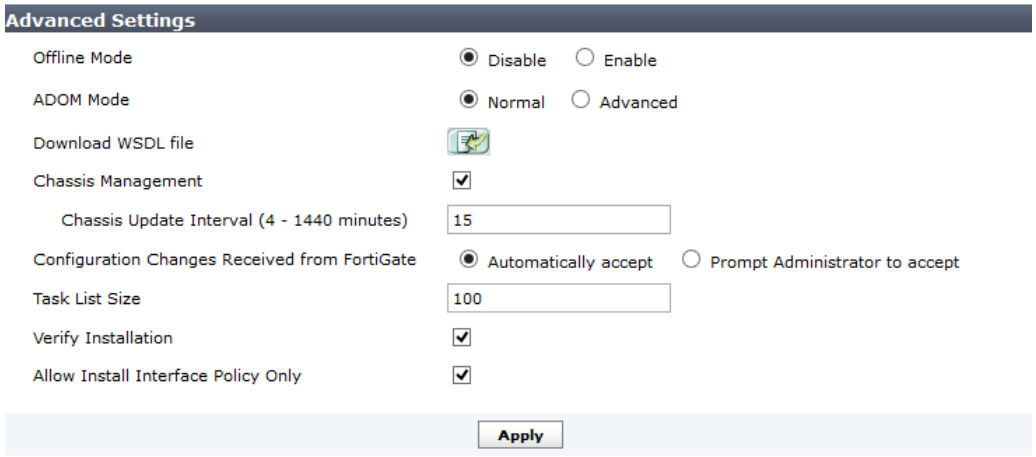
Configure the following settings and then select *Apply*:

Rollover Options	
Roll log file when size exceeds...	Enter the size, in megabytes, that the log file can be before it is rolled. Maximum allowed log file size is 500MB.
Roll log files at regular time	Select to roll the log file at a regular time. If selected: • Select to roll the logs on a weekly or daily basis from the drop-down menu • Select the hour and minute to roll the log files from the drop-down menus.
Enable log uploading	Select to upload real-time logs.
Upload Server Type	Select one of *FTP*, *SFTP*, or *SCP*.
Upload Server IP	Enter the IP address of the upload server.
Username	Select the username that will be used to connect to the server.
Password	Select the password that will be used to connect to the server.
Remote Directory	Select the remote directory on the 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 log files from the FortiManager system after they have been uploaded to the server.

Advanced Settings

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

Figure 72: Advanced settings



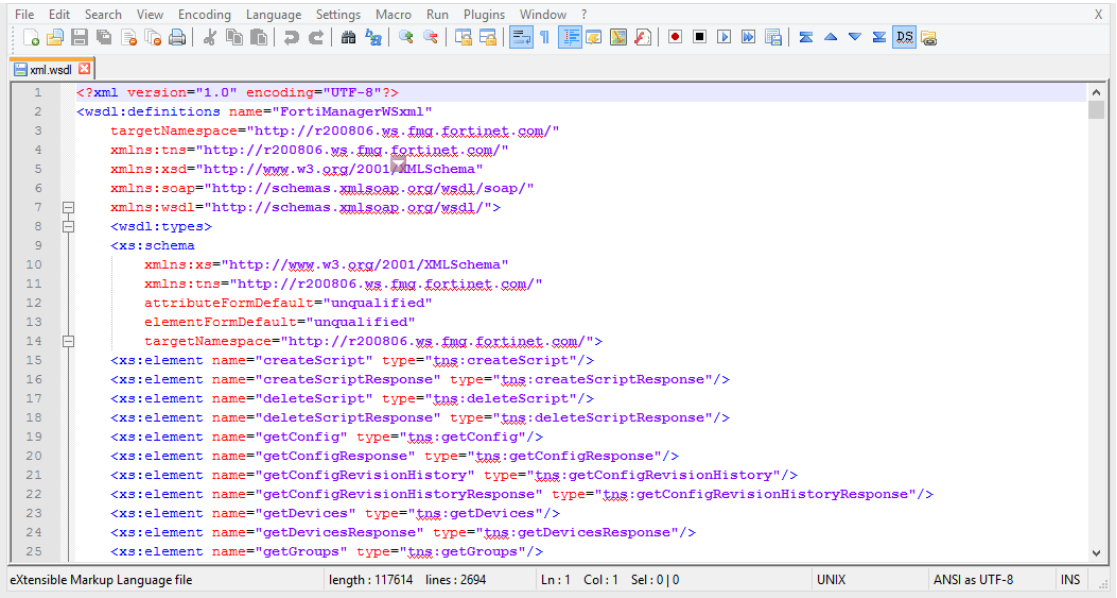
Configure the following settings and then select *Apply*:

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.
ADOM Mode	Select the ADOM mode, either *Normal* or *Advanced*.
Download WSDL file	Select to download the FortiManager unit's Web Services Description Language (WSDL) file. Web services is a standards-based, platform independent, access method for other hardware and software APIs. The file itself defines the format of commands the FortiManager will accept as well as the response to expect. Using the WSDL file, third-party or custom applications can communicate with the FortiManager unit and operate it or retrieve information just as an admin user would from the Web-based Manager or CLI.
Chassis Management	Enable chassis management.
Chassis Update Interval	Enter a chassis update interval from 14 to 1440 minutes (default is 15). This option is only available if chassis management is enabled.
Device Synchronization	Select to enable FortiManager to synchronize the settings you make with the managed devices.
Interval for synchronization	Select the time interval in minutes between synchronizations with devices.
Task List Size	Set a limit on the size of the task list.

Verify Installation	Select to preview the installation before proceeding.
Allow Install Interface Policy Only	Select to manage and install interface based policies only instead of all device and policy configuration.

Download the WSDL file for use with FortiManager XML API.

Figure 73:WSDL file



Device Manager

Use the Device Manager tab to view and configure managed devices. The Device Manager tab also provides access to scripts, and web portal features. For more information on script and web portal features see “Advanced Features” on page 242.

This chapter covers navigating the Device Manager tab, viewing devices, managing devices, managing access points, provisioning profiles, and managing certificate templates. For information on adding devices, and installing policy packages see “FortiManager Wizards” on page 206.



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

Device Manager tab

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

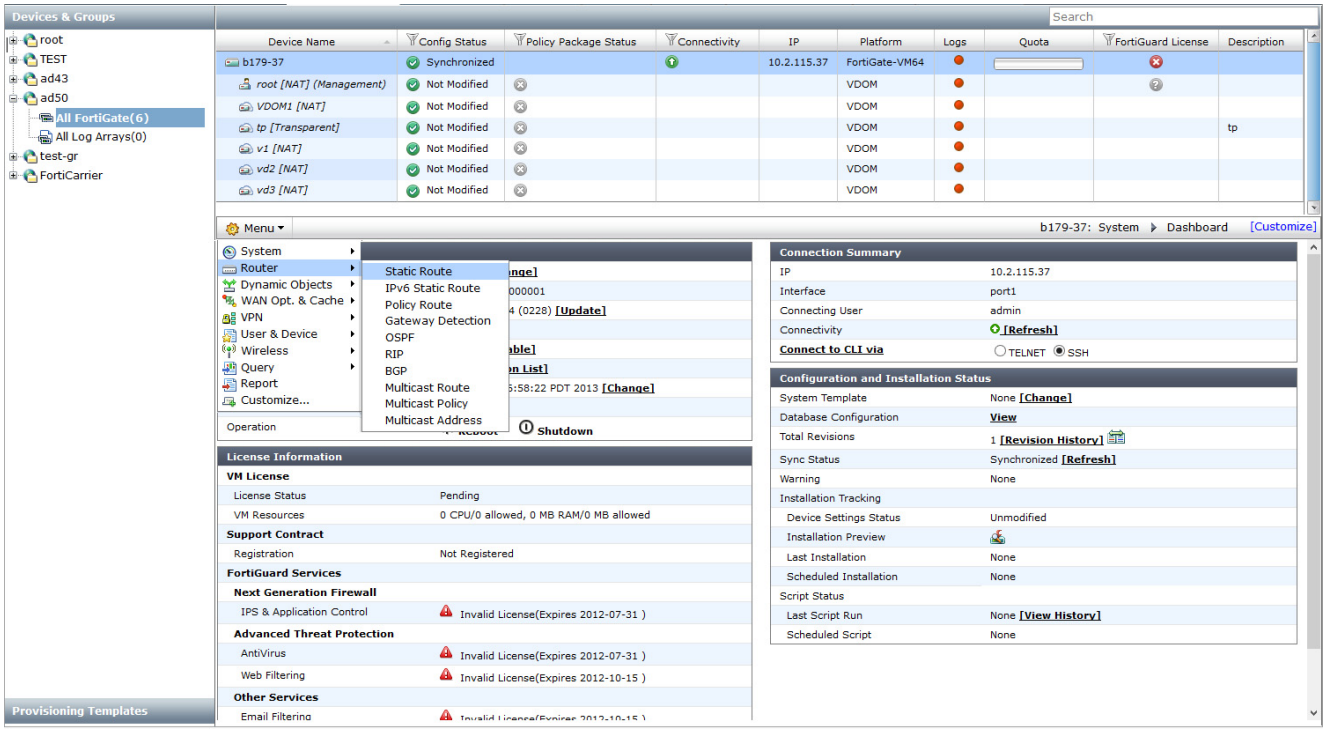
- Device Manager tab layout
- Device policy package status
- Device profiles
- Wireless profiles
- Extend workspace to entire ADOM
- Quick install

Device Manager tab layout

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

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

Figure 74: Device Manager layout



The top portion of the content pane shows the device list. When you select one of the devices in the table, the bottom portion of the content pane displays the selected device dashboard. The menu navigation of the device settings is in a menu format and referred to as the dashboard toolbar.



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

Device policy package status

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

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

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

Device profiles

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

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

Device profiles will support the following settings:

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

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

Device profiles can be found in the *Provisioning Profiles* tree menu on the Device Manager tab. See "System Templates" on page 177 for more information.

Wireless profiles

A wireless profile is a subset of a model device configuration. Each FortiAP device or group can be linked with a wireless profile. For more information, see "WiFi Templates" on page 179.

Extend workspace to entire ADOM

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

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

To enable and disable workspaces:

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

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

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



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

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

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

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

Quick install

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

Viewing managed device

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

This section contains the following topics:

- Using column filters
- View managed devices
- Dashboard widgets

Using column filters

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

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

Table 10: Column filters

Column	Filters
Device Name	Filter by device name (alphabetic).
Config Status	Filter by configuration status: • Synchronized • Synchronized from Auto Update • Out of Sync • Pending • Warning

Table 10: Column filters (continued)

Column	Filters
Policy Package Status	Filter by policy package status: • Installed • Never Installed • Modified
Connectivity	Filter by connectivity status: • Connected • Connection Down • Unknown
IP	Filter by IP (numeric).
Platform	Filter by platform type (alphabetic).
Logs	Filter by devices with logs.
Quota	Filter by device quota.
Log Connection	Filter by log connection status.
FortiGuard License	Filter by license status: • Valid • Expired • Unknown
Firmware Version	Filter by firmware version.
Other	Filter by Description, Contact, City, Province, Country, Company.

View managed devices

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

To view managed devices:

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

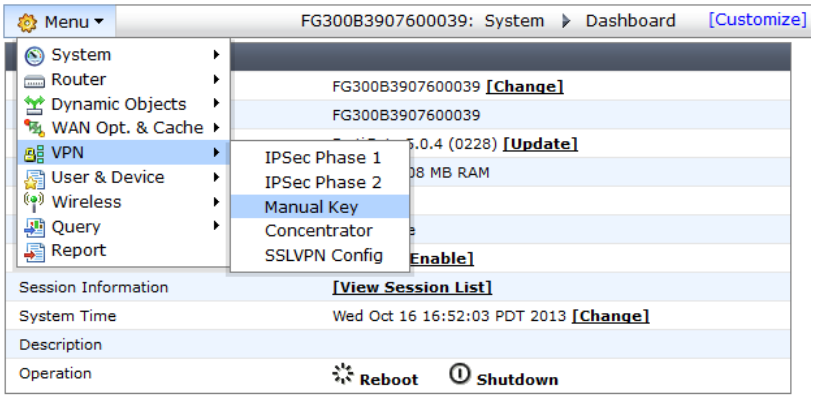
   The device dashboard and related information is shown in the lower content pane.

Dashboard toolbar

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

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

Figure 75: Device panel categories



The available panels can be customized at both the ADOM and device level.

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

Select *[Customize]* in the dashboard toolbar to customize the available panels at the device level.

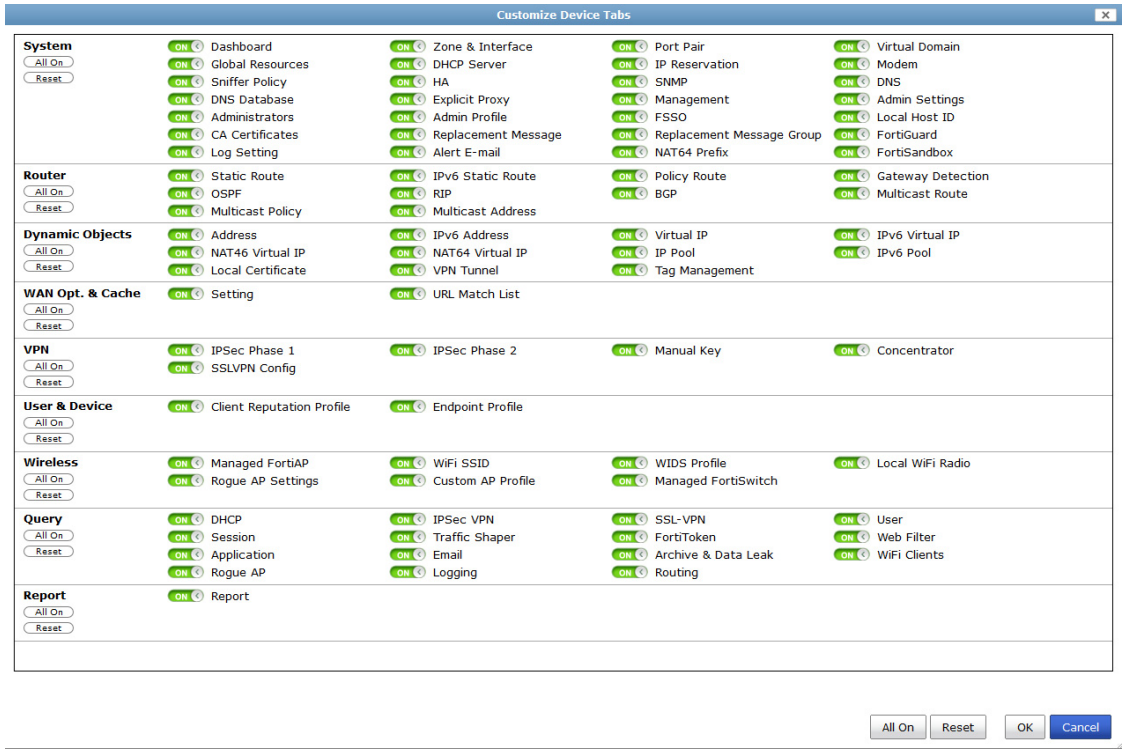


The options available on the dashboard toolbar will vary from device to device depending on what feature set the device supports. If a feature is not enabled on the device the corresponding tab will not be available on the toolbar.



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

Figure 76: Customize tabs



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

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

The following table provides an overview and descriptions of common dashboard toolbar panels, and content options.

System	
Dashboard	View device dashboard widgets including: • *System Information*: View device hostname, serial number, update firmware, enable VDOMs, and change system time. • *License Information*: View support contract and other device license information. • *Connection Summary*: Refresh connectivity and connect to the device CLI via TELNET or SSH. • *Configuration and Installation Status*: Change the system template, view database configuration, view revisions, refresh sync status, installation preview, and view script history. For more information, see "Dashboard widgets" on page 142.
Zone & Interface	Configure interfaces, VDOM links, zone mapping for interfaces, and intra-zone traffic. For more information, see "Zone & Interface" on page 145.
Port Pair	Configure port pairs for transparent VDOMs.

Virtual Domain	Configure virtual domains. Set the management virtual domain.
Global Resources	Select to view virtual domain resources. Left-click on a resource entry to configure settings. Right-click a resource entry to reset the value to default.
DHCP Server	Configure DHCP server and relay service settings. Column settings include *Interface, Type, Options, Enable,* and *Last Modified*.
IP Reservation	Configure regular and IPsec IP/MAC address reservations. Column settings include *IP, MAC Address, Type,* and *Last Modified*.
Modem	Enable and configure USB modem settings including up to three dialup accounts.
Sniffer Policy	Configure sniffer policies.
HA	View high availability configuration and cluster settings.
SNMP	Create new, enable, disable, and view SNMP v1, v2c, v3 Agent and Community configuration.
DNS	Configure IPv4 and IPv6 DNS or FortiGuard DDNS settings.
DNS Database	Create new, edit, and delete DNS zones. Column settings include *Name, Domain, TTL,* and *Last Modified*.
Explicit Proxy	Configure explicit web proxy options. Create new web proxy forwarding servers. Configure explicit FTP proxy options.
Management	Configure the management IP address and netmask.
Admin Settings	Configure Central Management, Web Administration Ports, Timeout Settings, Web Administration, and LCD Panel.
Administrators	Create new, edit, and delete administrators. Column settings include *Name, Trusted Hosts, Permission, Type, Virtual Domain, Two-factor Authentication,* and *Last Modified*.
Admin Profile	Configure administrator access profiles. Configure as global or VDOM, and set WiFi access. Column settings include *Name* and *Last Modified*.
FSSO	Configure FSSO agents and LDAP server settings. Column settings include *Name, FSSO Agent IP/Name, FSSO Group (s),* and *Last Modified*.
Local Host ID	Configure the local host ID. Advanced options include setting the tunnel SSL algorithm and the auto detect algorithm.
CA Certificates	Import, view, and delete CA certificates.

Replacement Messages	Configure replacement messages. You can configure replacement messages for the following categories: *Mail, HTTP, Web Proxy, FTP Proxy, FTP, NNTP, Alert Mail, Spam, Administration, Authentication, Captive Portal Default, FortiGuard Web Filtering, IM and P2P, Endpoint NAC, NAC Quarantine, Traffic Quota Control, SSL VPN,* and *Security*.
FortiGuard	Configure FortiGuard Distribution Network (FDN) services and settings.
Messaging Servers	Configure SMTP server settings.
Log Setting	Configure logging, and archiving settings. Enable event logging, and specify the types of events to log. You can select to enable memory logging, send logs to FortiAnalyzer/FortiManager, or Syslog. For more information, see "Log Setting" on page 146.
Alert E-mail	Configure alert email settings.
NAT64 Prefix	Enable NAT64 prefix and configure NAT64 prefix and always synthesize AAAA records.
FortiSandbox	Enable Sandbox inspection and configure the IP address and notifier email of your FortiSandbox device.
Router	
Routing Table	Configure static routes.
Static Route	Configure static routes. Column settings include *ID, IP, Mask, Gateway, Interface, Distance, Priority, Comment,* and *Last Modified*.
IPv6 Static Route	Configure IPv6 static routes. Column settings include *ID, IP, Gateway, Interface, Distance, Priority,* and *Last Modified*.
Policy Route	Configure policy routes. Column settings include *ID, Incoming, Outgoing, Source, Destination,* and *Last Modified*.
Gateway Detection	Configure new dead gateway detection. Column settings include *Interface, Ping Server, Detect Protocol, Interval, Failover,* and *Last Modified*.
OSPF	Configure OSPF default information, redistribute. Create new areas, network, and interfaces.
RIP	Configure RIP version, add networks, create new interfaces.
BGP	Configure local AS and router ID. Add neighbors and networks.
Multicast Route	Enable multicast routing, add static rendezvous points, and create new interfaces.

Multicast Policy	Configure multicast policies.
Multicast Address	Configure multicast addresses. Column settings include *Name, IP Range, Interface, Comments, Tags,* and *Last Modified*.
Dynamic Objects	Configure tags for tag management.
Address	Configure dynamic to local address mappings. Column settings include *Dynamic Address, Address / FQDN, Comments,* and *Last Modified*.
IPv6 Address	Configure IPv6 dynamic to local address mappings. Column settings include *Dynamic Address, Address / FQDN, Comments,* and *Last Modified*.
Virtual IP	Configure dynamic virtual IP to local virtual IP mappings. Column settings include *Dynamic Virtual IP, External Interfaces, IP, Service Port, Map to IP, Map to Port, Comments,* and *Last Modified*.
IPv6 Virtual IP	Configure IPv6 dynamic virtual IP to local virtual IP mappings. Column settings include *Dynamic Virtual IP, IP, Service Port, Map to IP, Map to Port, Comments,* and *Last Modified*.
NAT46 Virtual IP	Configure NAT64 dynamic virtual IP to local virtual IP mappings. Column settings include *Dynamic Virtual IP, IP, Service Port, Map to IP, Map to Port, Comments,* and *Last Modified*.
NAT64 Virtual IP	Configure NAT64 dynamic virtual IP to local virtual IP mappings. Column settings include *Dynamic Virtual IP, IP, Service Port, Map to IP, Map to Port, Comments,* and *Last Modified*.
IP Pool	Configure dynamic IP pool to local IP pool mappings. Column settings include *Dynamic IP Pool, Interface, Start IP, End IP, Comments,* and *Last Modified*.
IPv6 Pool	Configure dynamic IPv6 pool to local IP pool mappings. Column settings include *Dynamic IP Pool, Start IP, End IP, Comments,* and *Last Modified*.
Local Certificates	Configure dynamic local certificate to VPN local certificate mappings. Column settings include *Dynamic Local Certificate, VPN Local Certificate, Description,* and *Last Modified*.
VPN Tunnel	Configure dynamic VPN tunnel to VPN tunnel mappings. Column settings include *Dynamic VPN Tunnel, VPN Tunnel, Description,* and *Last Modified*.
Tag Management	Configure Tag Management.

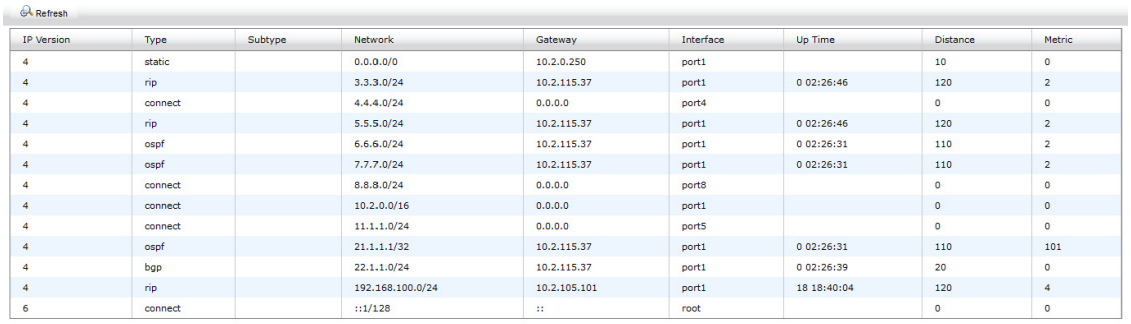
WAN Opt. & Cache	
Local Host ID	Configure the local host ID.
Rule	Configure WAN optimization rules.
Peer	Configure WAN optimization peers.
Authentication Group	Configure authentication groups.
Setting	Configure cache options.
URL Match List	Create, view, edit, and delete URL match entries. Column settings include *Name, URL Pattern, Forward Server, Cache Exemption, Comments, Status,* and *Last Modified*.
Exempt List	Configure exempt URLs.
VPN	
IPsec Phase 1	Configure IPsec Phase 1 settings. Create FortiClient VPN.
IPsec Phase 2	Configure IPsec Phase 2 settings.
Manual Key	Configure manual key settings.
Concentrator	Configure concentrator settings. Column settings include *Concentrator Name, Members,* and *Last Modified*.
SSLVPN Config	Configure SSL VPN settings including DNS and WINS servers.
User & Device	
Endpoint Profile	Create, view, edit, and delete endpoint profiles.
Client Reputation Profile	Create, view, edit, and delete client reputation profiles.
Wireless	
Managed FortiAP	Discover and authorize FortiAP devices. View managed FortiAP settings. Column settings include *State, Name, Serial Number, SSIDs, AP Profile,* and *Last Modified*.
WiFi SSID	Configure WiFi SSID.
WIDS Profile	Configure wireless intrusion detection system (WIDS) profiles.
Rogue AP Settings	Enable or disable rogue AP detection and on-wire rogue AP detection technique.
Local WiFi Radio	Configure the local radio.
Custom AP Profile	Configure AP profiles.

Query	
DHCP	DHCP query for the device selected including *Interface, IP, MAC address, VCI, expiry* and *Status*.
IPsec VPN	IPsec VPN query for the device selected including *Name, Type, User Name, Incoming Data, Outgoing Data, Gateway, Port, Source Proxy, Destination Proxy, Status, P2 Name, P2 SN, Timeout,* and *Up Time*. You can change the status of a connection from this tab.
SSL-VPN	SSL-VPN query information for the device selected including *User Name, Remote Host, Last Login Time, Subsession Type* and *Subsession Description*.
User	User query for the device selected including *User Name, User Group, Policy ID, Duration, Expiry, Traffic Volume* and *Method*. You have the option to de authorize a user.
Session	Session query information for the device selected.
Traffic Shaper	Traffic Shaper query information for the device selected.
FortiToken	FortiToken query for the device selected including the *Serial Number* and *Status*. You can activate a FortiToken from this tab.
Web Filter	Web filter query for the device selected including *Protocol, Requests, Quarantined, Email Filter, Banned Word, File Filter, AntiVirus, Archive, FortiGuard, URL Filter,* and *Fragmented*.
Application	Application query for the device selected including *ID, Bytes, Application Name* and *Sessions*.
Email	Email query for the device selected including *Protocol, Requests, Email Filter, Banned Word, File Filter, AntiVirus, Archive, FortiGuard, URL Filter* and *Fragmented*.
Routing	Routing query for the device selected including *IP Version, Type, Subtype, Network, Gateway, Interface, Up Time, Distance,* and *Metric*.
Archive & Data Leak	Archive and data leak queries for the device selected.
WiFi Clients	WiFi client query including *IP, SSID, FortiAP, MAC Address, Authentication, Vendor Info, Rate, Signal Strength, Idle Time, Association Time,* and *Bandwidth Tx/Rx*.
Rogue AP	Rogue AP query including *State, Online Status, SSID, MAC Address, Vendor Info, Security Type, Signal Strength, Channel, Rate, First Seen, Last Seen, Detected By,* and *On-Wire*. You have the option to change the status of a connection from this tab.
Logging	Logging queries.
Report	
Report	View, download, and delete device reports.

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

Figure 77 provides an example of the routing query output.

Figure 77: Routing query output



IP Version	Type	Subtype	Network	Gateway	Interface	Up Time	Distance	Metric
4	static		0.0.0.0/0	10.2.0.250	port1		10	0
4	rip		3.3.3.0/24	10.2.115.37	port1	0 02:26:46	120	2
4	connect		4.4.4.0/24	0.0.0.0	port4		0	0
4	rip		5.5.5.0/24	10.2.115.37	port1	0 02:26:46	120	2
4	ospf		6.6.6.0/24	10.2.115.37	port1	0 02:26:31	110	2
4	ospf		7.7.7.0/24	10.2.115.37	port1	0 02:26:31	110	2
4	connect		8.8.8.0/24	0.0.0.0	port8		0	0
4	connect		10.2.0.0/16	0.0.0.0	port1		0	0
4	connect		11.1.1.0/24	0.0.0.0	port5		0	0
4	ospf		21.1.1.1/32	10.2.115.37	port1	0 02:26:31	110	101
4	bgp		22.1.1.0/24	10.2.115.37	port1	0 02:26:39	20	0
4	rip		192.168.100.0/24	10.2.105.101	port1	18 18:40:04	120	4
6	connect		::1/128	::	root		0	0

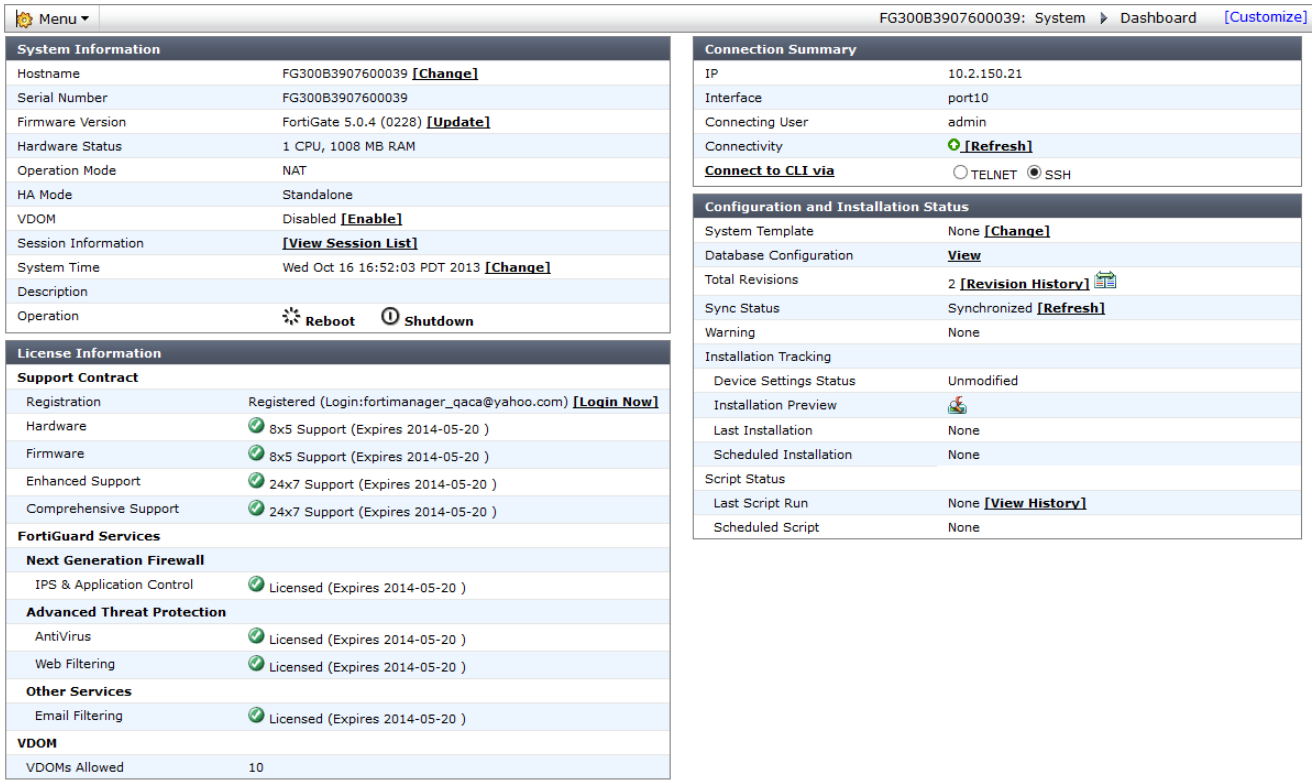
For information on configuring FortiGate settings locally on your FortiManager device, see the *FortiOS 5.0 Handbook*.

Dashboard widgets

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

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

Figure 78: FortiGate unit dashboard



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

System Information	
Hostname	The name of the device. Select *Change* to change the name.
Serial Number	The device serial number.
Firmware Version	The device firmware version and build number. Select *Update* to view and update the device firmware.
Hardware Status	The number of CPUs and the RAM size.
License Status	The license status (VM only).
VM Resources	The number of CPU's installed, and allowed. The amount of RAM installed, and allowed (VM only).
Operation Mode	Operational mode of the FortiGate unit: NAT or Transparent.

HA Mode	Standalone indicates non-HA mode. Active-Passive, Active-Active indicates the device is operating in a cluster. Select *Details* to view cluster settings.
Cluster Name	The name of the cluster.
Cluster Members	The hostname, serial number, role, and status of cluster members.
VDOM	The status of VDOMs on the device. Select *Enable*/*Disable* to toggle the VDOM role.
Session Information	Select *View Session List* to view the device session information.
System Time	The device system time and date information. Select *Change* to set time or synchronize with NTP server.
Description	Descriptive information about the device.
Operation	Select to *Reboot* or *Shutdown* the managed device.
License Information	
VM License	The VM license status and resources.
Support Contract	The support contract information and the expiry date. The support contract includes the following: Registration, Hardware, Firmware, and Support Level e.g. Enhanced Support, Comprehensive Support.
FortiGuard Services	The contract version, issue date and service status. FortiGuard Services includes the following: Antivirus, Intrusion protection, Web filtering, and Email filtering.
VDOM	The number of virtual domains that the device supports.
Connection Summary	
IP	The IP address of the device.
Interface	The port used to connect to the FortiManager system.
Connecting User	The user name for logging in to the device.
Connectivity	The device connectivity status and the time it was last checked. A green arrow means that the connection between the device and the FortiManager system is up; a red arrow means that the connection is down. Select *Refresh* to test the connection between the device and the FortiManager system.
Connect to CLI via	Select the method by which the you connect to the device CLI, either SSH or TELNET.
Configuration and Installation Status	
Device Profile	The device profile associated with the device. Select *Change* to set this value.

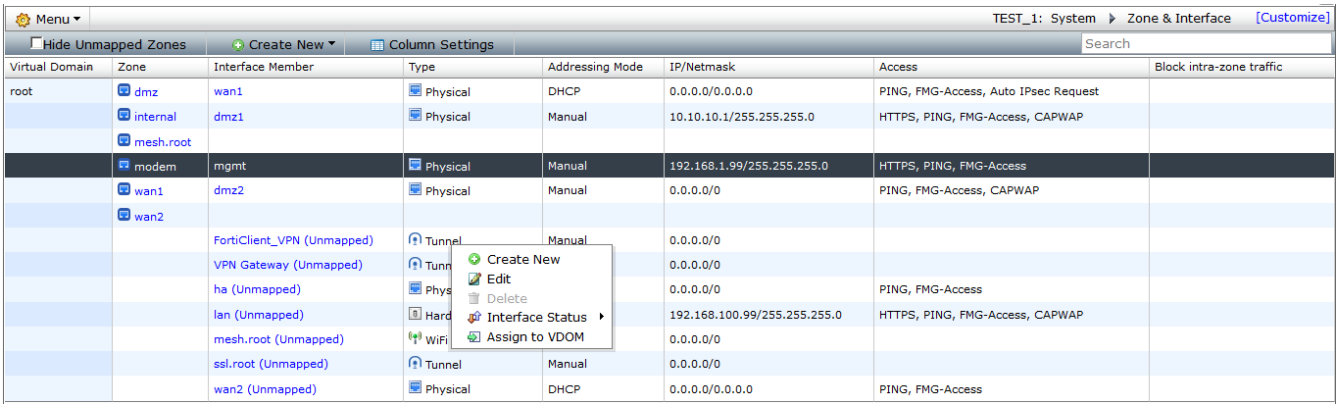
Database Configuration	Select *View* to display the configuration file of the FortiGate unit.
Total Revisions	Displays the total number of configuration revisions and the revision history. Select *Revision History* to view device history.
Sync Status	The synchronization status with the FortiManager.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

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

Zone & Interface

The *Zone & Interface* page provides access to device level zone and interface information. On this page you can create interfaces and VDOM links.

Figure 79: Zone & Interface page



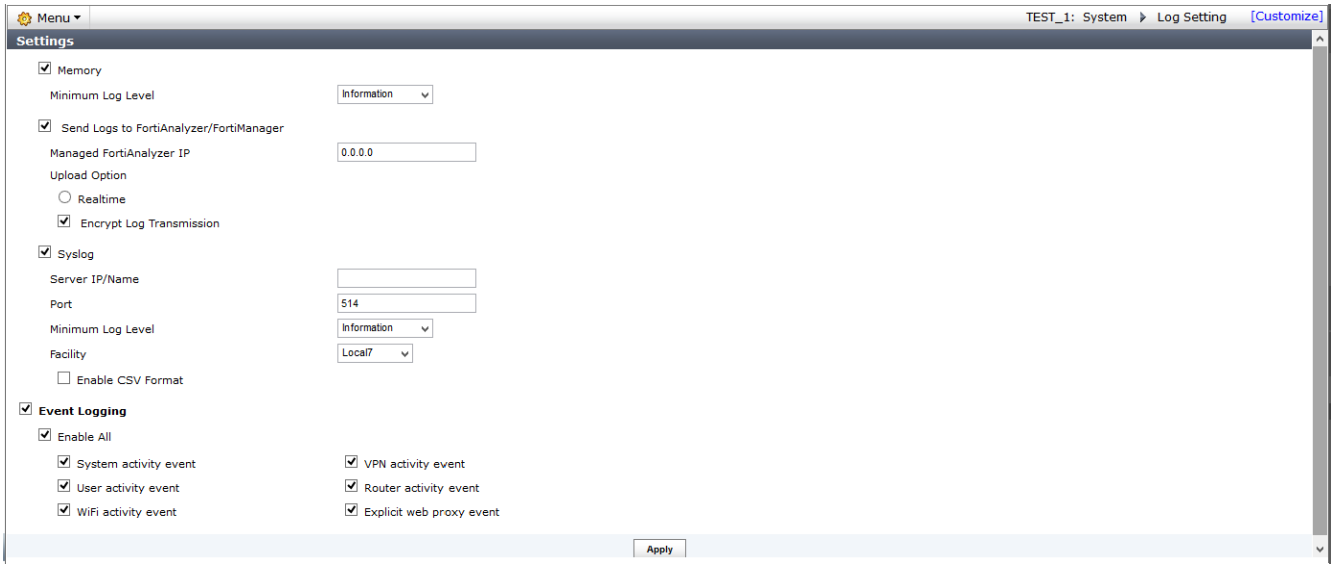
The following table lists the information and available options available on the *Zone & Interface* page:

Hide Unmapped Zones	Select to show or hide unmapped zones.
Create New	Select to create a new interface or VDOM link.
Column Settings	Column settings include the following: VLAN ID, Alias, Description, Administrative Status, Rx (Bytes), Tx (Bytes), Total (Bytes), Rx (Packets), Tx (Packets), Rx (Error), Tx (Error), Total (Error), Secondary IP, MTU, Virtual Domain, Zone, Interface Member, Type, Addressing Mode, IP/Netmask, Access, IPv6 IP/Netmask, IPv6 Access, Block intra-zone traffic, and Last Modified.
Search	Use the search field to find and display specific content.
Create New	Select *Create New* in the right-click menu to create a new interface.
Edit	Select an entry in the table, right-click, and select *Edit* in the menu to edit the entry.
Delete	Select an entry in the table, right-click, and select *Delete* in the menu to delete the entry.
Interface Status	Select an entry in the table, right-click, and select *Interface Status* in the menu and select the interface status as up or down.
Assign to VDOM	Select an entry in the table, right-click, and select *Assign to VDOM* in the menu and select the VDOM in the *Assign to VDOM* dialog box.

Log Setting

On the *Log Setting* page you can configure device logging to memory, to FortiAnalyzer / FortiManager and to Syslog. You can also enable event logging and select which events to log.

Figure 80: Log Setting page



The following table lists the information and available options available on the *Log Setting* page:

Memory	Select to enable memory logging and select the minimum log level from the drop-down list.
Send Logs to FortiAnalyzer/FortiManager	Select to send logs to FortiAnalyzer/FortiManager, enter the managed FortiAnalyzer IP address (optional), and select the upload option. You can also select to encrypt log transmission.
Syslog	Select to enable syslog logging, enter the server IP/name, port, minimum log level, and facility. You can also select to enable CSV format logs.
Event Logging	Select to enable event logging and select the event types to log.

Unregistered devices

In FortiManager v5.0 Patch Release 4 or earlier releases, the `config system global set unregister-pop-up` command is enabled by default. When a device is configured to send logs to FortiManager, the unregistered device table will be displayed. You can decide to add devices to specific ADOMs now, at a later date, or delete the device.

In FortiManager v5.0 Patch Release 5 or later, the `config system global set unregister-pop-up` command is disabled by default. When a device is configured to send logs to FortiManager, the unregistered device table will not be displayed. Instead, a new entry *Unregistered Devices* will appear in the Device Manager tab under *All FortiGate*. You can then promote devices to specific ADOMs or use the right-click menu to delete the device.

Administrative domains (ADOMs)

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

- Firmware version: group all v5.0 devices into one ADOM, and all v4.0 MR3 into another.
- Geographic regions: group all devices for a specific geographic region into an ADOM, and devices for a separate region into another ADOM.
- Admin users: group devices into separate ADOMs based for specific administrators responsible for the group of devices.
- Customers: group all devices for one customer into an ADOM, and devices for another customer into another ADOM.
- FortiMail, FortiWeb, FortiSwitch, and FortiCarrier devices are automatically placed in their own ADOMs.

Each admin profile can be customized to provide read-only, read-write, or restrict access to various ADOM settings. When creating new admin accounts, you can restrict which ADOMs the administrator can access, for enhanced control of your admin users. For more information on ADOM configuration and settings, see "Administrative Domains" on page 48.



For information on adding devices to an ADOM using the *Add Device* wizard, see "FortiManager Wizards" on page 206.

Managing devices

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

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

This section includes the following topics:

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

Adding a device

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

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

provision a new device which is not yet online, use the *Add Device* wizard, but select *Add Model Device* instead of *Discover*.

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

To add a device to an ADOM:

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



For detailed information on adding devices to an ADOM using the *Add Device* wizard, see "FortiManager Wizards" on page 206.

Replacing a managed device

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



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

View all managed devices from the CLI

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

```
diagnose dvm device list
```

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

Figure 81: View all managed devices from the CLI

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

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

FMG-VM64 #
```

Changing the serial number from the CLI

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

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

This command is also useful when performing an RMA replacement.

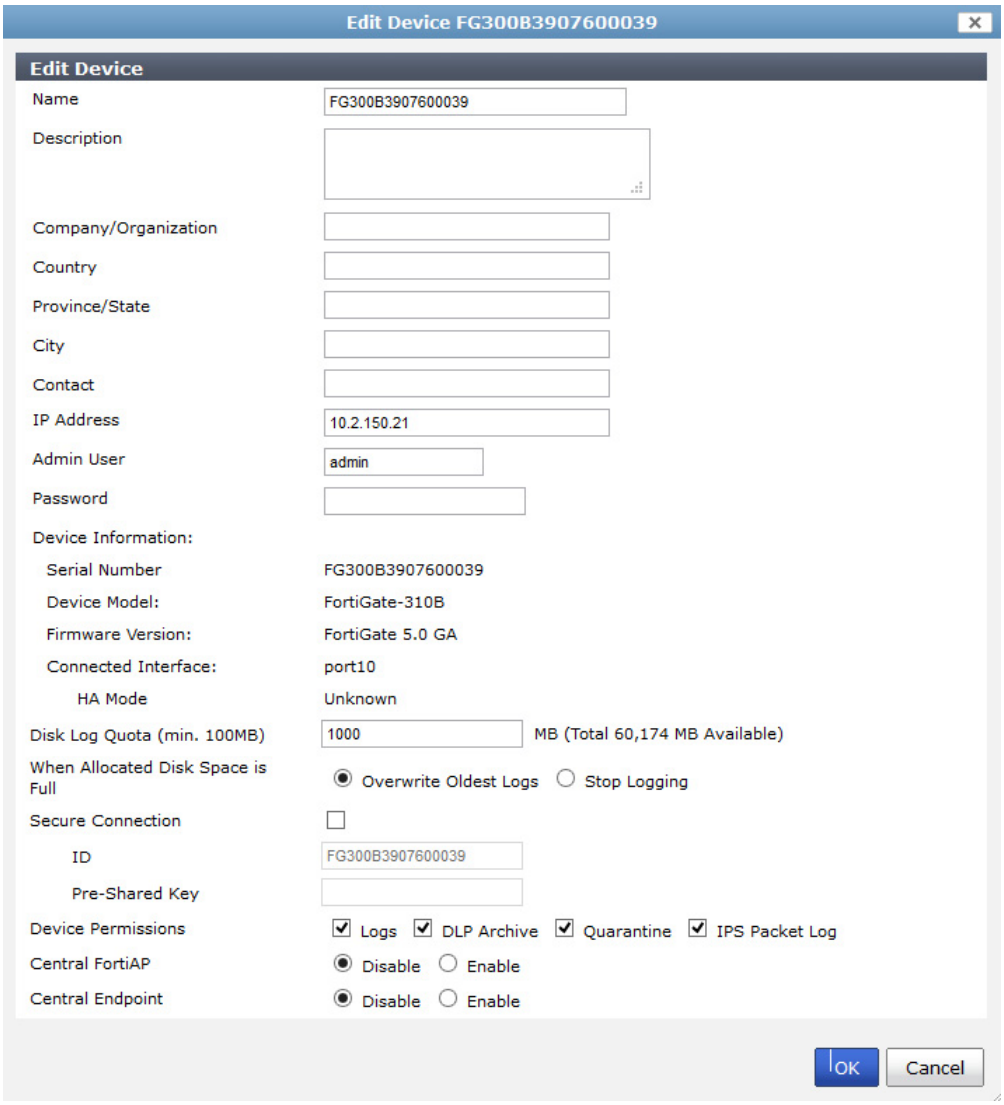
Editing device information

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

To edit information for a single device:

1. On the tree menu, select the ADOM, and device group.
2. Right-click on the device row and select *Edit* from the right-click context menu.

Figure 82: Edit a device



3. Edit the following settings as required.

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

Province/State	Enter the province or state.
City	Enter the city.
Contact	Enter the contact name.
IP Address	The IP address of the device.
Admin User	The admin user username.
Password	The admin user password
Device Information	Information about the device, including serial number, device model, firmware version, connected interface, HA mode, cluster name, and cluster members.
Disk Log Quota	The amount of space that the disk log is allowed to use, in MB. The minimum value is 100MB. The maximum value depends on the device model and available disk space.
When Allocated Disk Space is Full	The action for the system to take when the disk log quota is filled.
Secure Connection	Select check box to enable this feature. Secure Connection secures OFTP traffic through an IPsec tunnel.
ID	The ID is the device serial number.
Pre-Shared Key	The pre-shared key for the IPsec connection between the FortiGate and FortiManager.
Device Permissions	The device's permissions.
Central FortiAP	Enable or disable central FortiAP.
Central Endpoint	Enable or disable central Endpoint.

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



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



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

See also

- Importing and exporting device lists

Refreshing a device

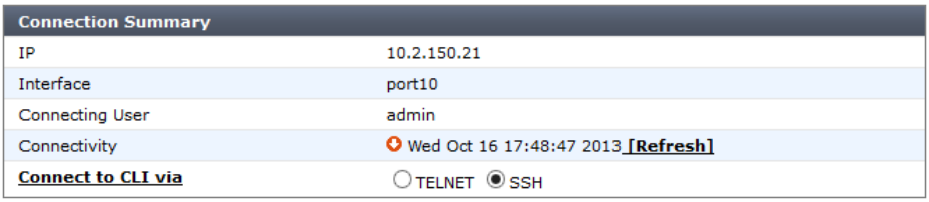
Refreshing a device refreshes the connection between the selected devices and the FortiManager system. This operation updates the device status and the FortiGate HA cluster member information.

To refresh a device:

1. In the content pane, right-click on the device.
2. Select *Refresh* from the po-up menu.

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

Figure 83: Connection Summary widget



Install policy package and device settings

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

To import policies to a device:

1. Right-click on the tree menu device entry, and select *Install* on the context menu.

   The *Install Wizard* will appear.
2. Select *Install Policy Packages & Device Settings*.

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



For information on importing policy packages and device settings to a device using the *Install* wizard, see "FortiManager Wizards" on page 206.

Importing and exporting device lists

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



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



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

There are two ways to create the text file:

- *Export Device List*: Use this feature to save a list of devices in a text file as a backup that can be imported later.
- Create the file manually: For more information, see “Example text files” on page 157.

To import a device list:

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

To export a device list:

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

Import text file general format

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

```
device_list_ver=8
```

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

ADOM file format

ADOMs are specified by the following ADOM lines:

```
device_list_ver=8
adom|name|mode|status|version|mr|migration_mode|enable|
```

One or more “+meta” lines may follow a ADOM line to specify the values of metadata associated with that ADOM. See “Metadata file format” on page 156.

Field Name	Blank Allowed	Description
name	No	Name of the ADOM.
mode	No	In FortiManager v5.0 the mode is GMS. This field reflects legacy code.
status	No	Enter 1 to enable the ADOM. Enter 0 to disable the ADOM.
version	No	The ADOM version, for example, 5.0.

mr	No	Major Release designation of the device. For example, GA, MR1, MR2.
migration mode	No	In FortiManager v5.0 the value is 0. This field reflects legacy code.
enable	No	Enter 1 to enable, 0 to disable.



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

Device file format

Devices are specified by the following device lines:

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

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

Field Name	Blank Allowed	Description
ip	No	Device IP address.
name	No	Device name.
platform	No	The device type. For example, FortiGate, or the full platform name: FortiWiFi-60B.
admin	No	Administrator username.
passwd	Yes	Administrator password.
adom	Yes	The ADOM into which this device should be imported. If this field is left blank, the device is imported into the current ADOM.
desc	Yes	Device description.
discover	No	Enter 1 to automatically discover device, 0 otherwise.
reload	No	Enter 1 to reload the device configuration after importing it, 0 otherwise.
fwver	No	Firmware version.
mr	No	Major Release designation of the device. For example, GA, MR1, MR2.
patch	No	Patch level.
build	No	The four digit build number

branch_pt	No	The firmware branch point. You can find this information from the FortiOS CLI command get system status.
sn	No	Device serial number.
has_hd	No	Enter 1 if the device has a hard disk, 0 if the device does not.
faz.quota	No	The disk log quota in MB.
faz.perm	No	The device permissions. *DVM_PERM_LOGS*: Permission to receive and store log messages *DVM_PERM_DLP_ARCHIVE*: Permission to receive and store DLP archive files *DVM_PERM_QUARANTINE*: Permission to receive and store quarantine files *DVM_PERM_IPS_PKT_LOG*: Permission to receive and store IPS packet log.

Following the device line, there may be one or more “+meta” lines specifying metadata for the device (For more information, see “Metadata file format” on page 156), 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.

Group file format

Device group are specified as follows:

```
device_list_ver=8
group|name|desc|adom|
```

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

One or more “+meta” lines describing metadata values for the group, or one or more lines describing group members and subgroups, may follow the group line. See see “Metadata file format” on page 156.

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

Field Name	Blank Allowed	Description
devname	No	Name of the device.
vdom	Yes	The VDOM of the device that belongs to this group. If this field is left empty, the VDOM refers to the root VDOM.
groupname	No	The name of the subgroup that belongs to this group.

Metadata file format

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

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

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

String transliterations

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

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

Example text files

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

Example 1: Device

```
device_list_ver=8
# Device definitions. The lines beginning with '+' are
# associated with the device, and will cause an error if they
# appear out-of-context.
device|10.0.0.74|top|FortiGate|admin||root|My description.|1|1|
+meta|bogosity|10|
+vdom|vdom01|root|
+vdom|vdom02|root|
+vdom|vdom03|root|
+vdom|vdom04|root|
device|10.0.0.75|bottom|FortiGate-400C|admin|password|adom01|Your
     description.|0|1|5.0|GA|FG400C2905550018|0|
+meta|bogosity|12|
+vdom|vdom01|adom01|
```

Example 2: ADOM

```
device_list_ver=8
# ADOM definitions. These are exported only from the root ADOM,
# and can only be imported in the root ADOM. Import will abort
# with an error if this is imported in a non-root ADOM.
# The lines beginning with '+' are associated with the
# last-defined ADOM, and will cause an error if they appear
# out-of-context.
adom|root|GMS|1|
+meta|tag|my domain|
adom|adom01|GMS|1|
+meta|tag|your domain|
```

Example 3: Device group

```
device_list_ver=8
# Group definitions. Groups will be created in the order they
# appear here, so subgroups must be defined first, followed by
# top-level groups. Only two levels of nesting are supported.
group|group01|My description.|root|
+member|bottom||
+member|top|vdom03|
group|group02|Another description.|root|
+meta|supervisor|Philip J. Fry|
+member|top|vdom01|
+member|top|vdom02|
+subgroup|group01|
group|group03||adom01|
+meta|supervisor|Bender B. Rodriguez|
```

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

Setting unregistered device options

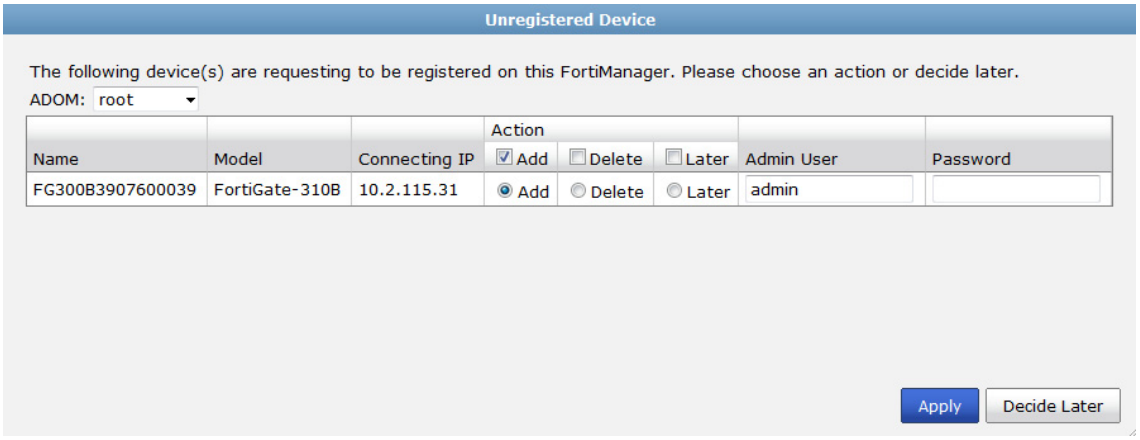
In FortiManager v5.0, setting unregistered device options is from the CLI only. Enter the following command to enable or disable allowing unregistered devices to be registered with the FortiManager.

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

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

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

Figure 84: Unregistered device dialog box on login



Configuring devices

You can configure the FortiGate units in three ways:

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

This section contains the following topics:

- Configuring a device
- Configuring virtual domains (VDOMs)

Configuring a device

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

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

To configure a FortiGate unit:

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

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



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

Firewall policy reordering on first installation

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

This behavior is normal for the following reasons:

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

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

This behavior would only be seen:

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

Configuring virtual domains (VDOMs)

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



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

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

Creating and editing virtual domains

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

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

To enable virtual domains:

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

To create a virtual domain:

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



The Virtual Domain tab may not be visible in the lower content pane tab bar. See “View managed devices” on page 133 for more information.

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

Figure 85: Create a new NAT VDOM

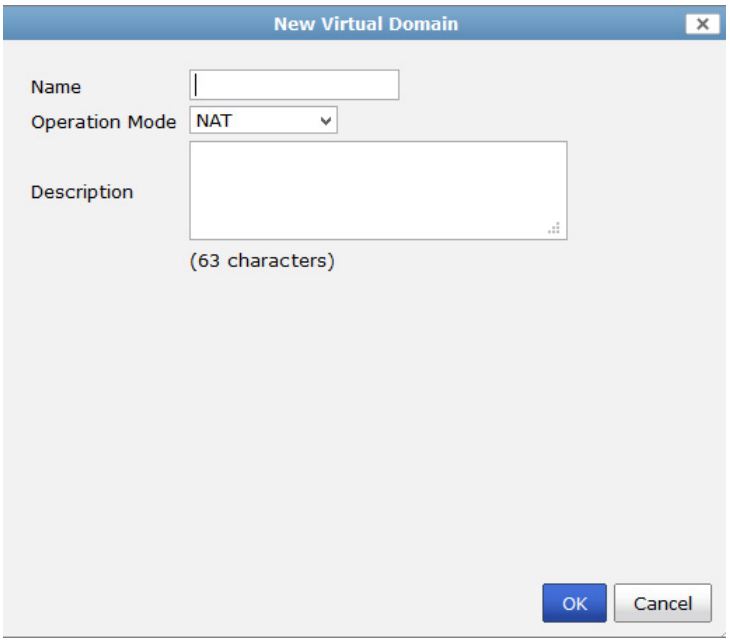
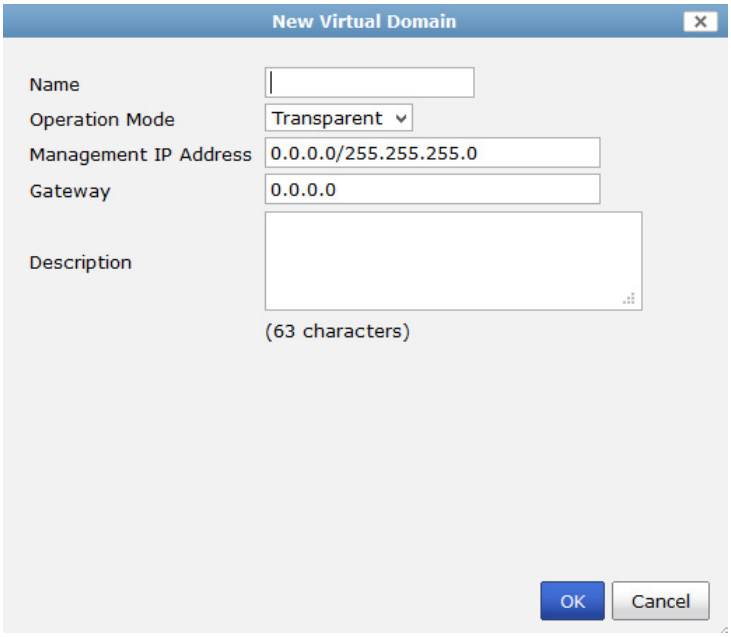


Figure 86: Create a new transparent VDOM



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

Configuring inter-VDOM routing

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

Before configuring inter-VDOM routing:

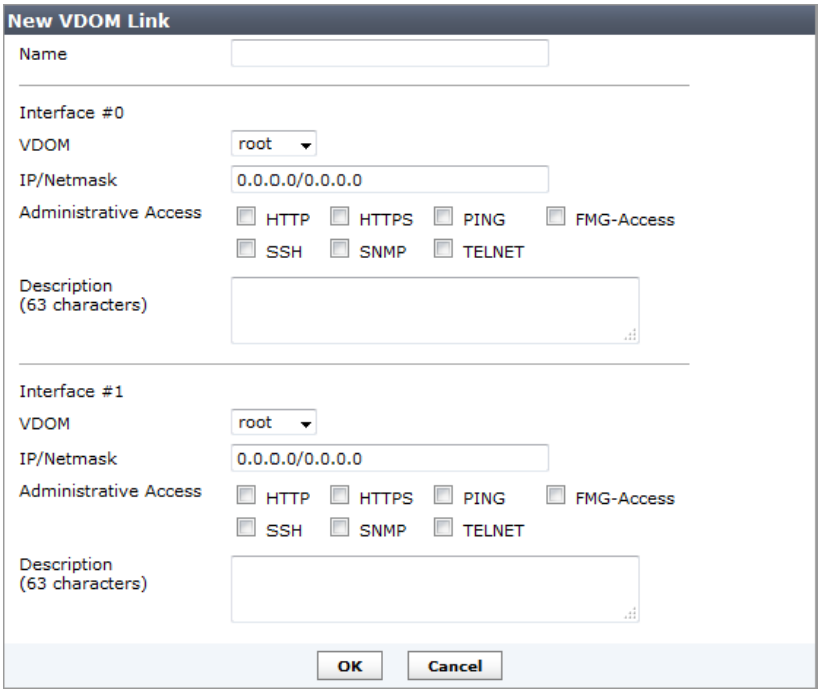
- You must have at least two virtual domains configured.
- The virtual domains must all be in NAT mode.
- Each virtual domain to be linked must have at least one interface or subinterface assigned to it.

To create a VDOM link:

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

   The *New VDOM Link* window opens.

Figure 87: New VDOM link



4. Enter the following information:

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

5. Select *OK* to save your settings.

Configuring VDOM resource limits

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

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

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

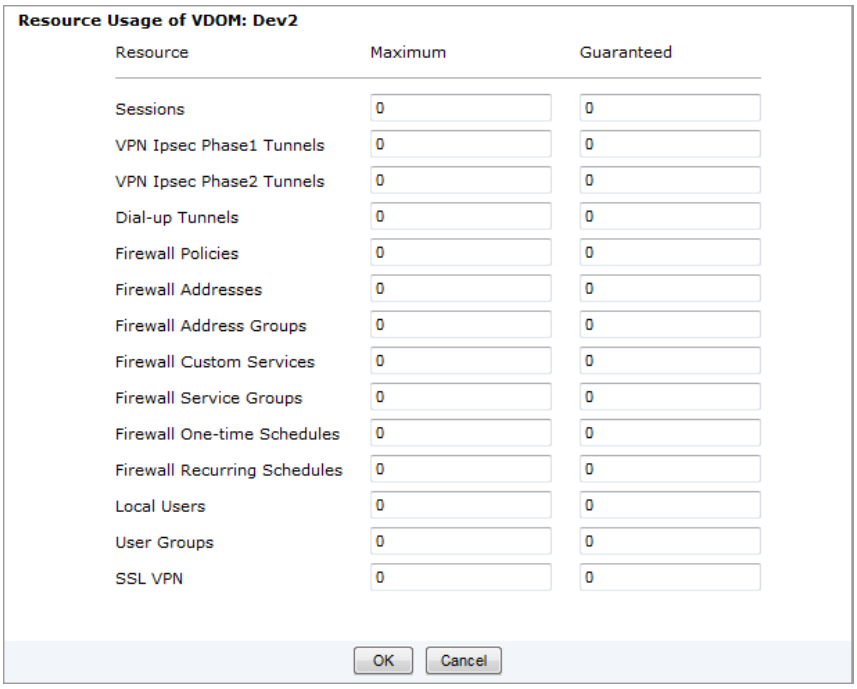
For more information, see "Configuring VDOM global resources" on page 164.

To configure a VDOM's resource limits:

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

   The *Resource Usage* page opens.

Figure 88: Resource usage page



3. For each resource:
   - enter the maximum value allowed for this resource. If you enter a wrong value, a warning appears with the correct value range.
   - enter the value allocated for this resource. This value must be lower than or equal to the maximum value.
4. Select *OK*.

Configuring VDOM global resources

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

To configure VDOM global resources:

1. In the Device Manager tab, select the unit you want to configure.
2. In the lower content pane, select the *Global Resources* tab.

Resource	The network resources that the VDOMs can use. Select the resource name to edit the configured value.
Configured Maximum	The maximum resource limit for all VDOMs set by the user. Unlimited is represented by a *0*.

Default Maximum	The default maximum resource limit for all VDOMs. Unlimited is represented by a *0*.
Reset	Right-click and select *Reset* to set the configured values to their default values.

Log arrays

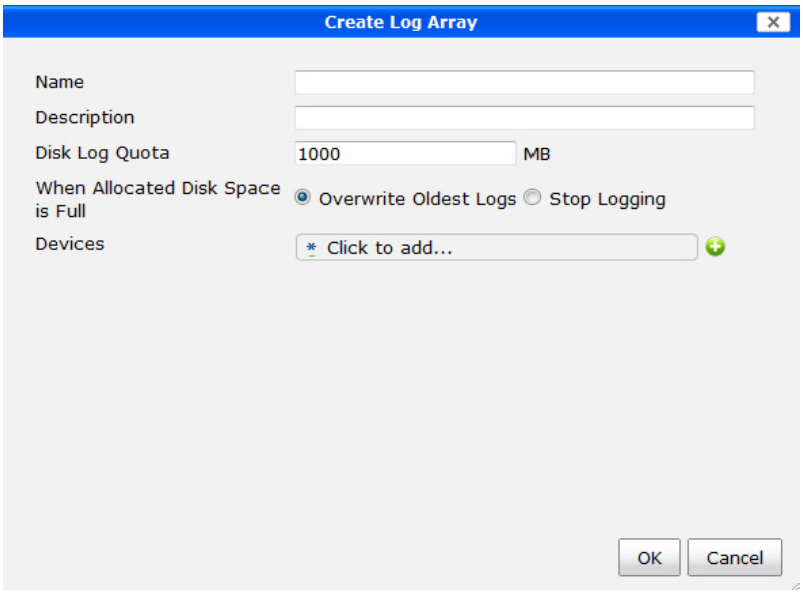
Log arrays support group-based access to logs and reports. Log arrays are available in the Device Manager tab. Log arrays also allow you to manage log data belonging to FortiGate HA clusters from a single device object. You can schedule reports for each log array.

It is recommended that you configure log arrays before deploying the FortiManager into production. When adding and deleting log arrays, you will need to rebuild the database to view older logs.

To create a new log array:

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

Figure 89: Create log array window



2. Configure the following settings:

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

3. Select *OK* to save the log array configuration.



After creating a log array, only new logs will be populated into it. Older logs will remain on the device. To collect older logs, you will need to rebuild the array database using the following CLI command:

```
execute sql-local rebuild-device <log array device ID>
```

The SQL logs for the members of the log array will be rebuilt. To verify that the array rebuild was successful, select the Log View tab and view the log array and logs.

To edit a log array:

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

To delete a log array:

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

Access points

Access points that are managed by the FortiGate units managed by the FortiManager device can be configure from the All FortiAP group in the tree menu of the Device Manager tab. Right-clicking on the FortiAP devices allows the devices to be edited, updated, and restarted; client and rogue AP lists can also be viewed.

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

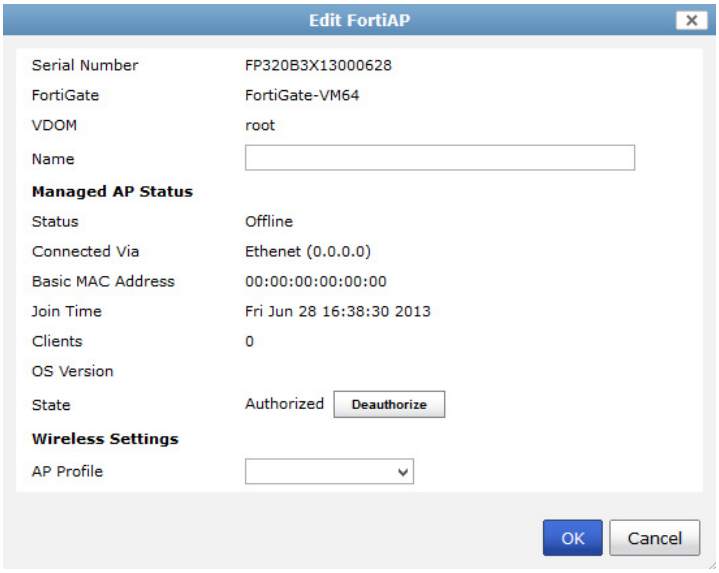
FortiGate	The FortiGate that is managing the FortiAP.
VDOM	The VDOM that contains the FortiAP.
Access Point	The access point.
Serial Number	The device's serial number.
State	The state of the FortiAP device. Hover the cursor over the icon to see a description of the state.
Connected Via	The method by which the device is connected to the FortiGate.
AP Profile	The AP Profile used by the device.
Join Time	The time that the device joined.
Channel	The channel or channels used by the device.
OS Version	The operating system version running on the device.

To edit a FortiAP device:

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

   The *Edit FortiAP* dialog box opens.

Figure 90: Edit FortiAP



2. Configure the following settings:

Serial Number	The device's serial number. This field cannot be edited.
FortiGate	The FortiGate that is managing the device. This field cannot be edited.
VDOM	The VDOM that contains the FortiAP. This field cannot be edited.
Name	Enter a name for the FortAP device.
Managed AP Status	
Status	The status of the FortiAP device, such as *Connected*. This field cannot be edited.
Connected Via	The method by which the device is connected to the FortiGate. This field cannot be edited.
Basic MAC Address	The MAC address of the device. This field cannot be edited.
Join Time	The time that the device joined. This field cannot be edited.
Clients	The number of clients connected to the device. This field cannot be edited.
OS Version	The operating system version being used by the device. This field cannot be edited.
State	Select *Authorize* or *Deauthorize* to authorize or deauthorize the device.

Wireless Settings	
AP Profile	Select an AP profile to apply to the device from the drop-down list. The list will be limited to profiles that correspond to the device model.

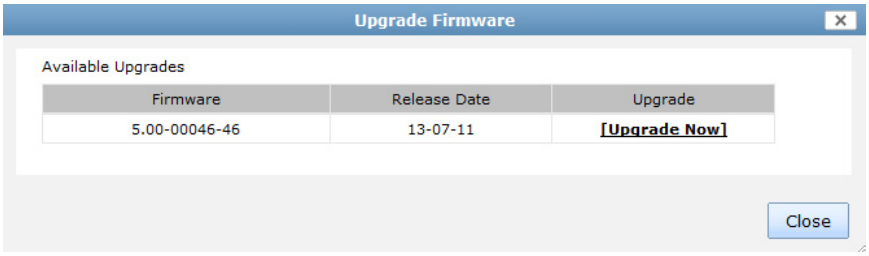
3. Select *OK* to save your changes.

To update the FortiAP device firmware:

1. Right-click on a device in the FortiAP list and select *Upgrade* from the pop-up menu.

   The *Upgrade Firmware* dialog box opens, listing the available updates.

   Figure 91: Upgrade firmware



2. Select *Upgrade Now*, and then select *OK* in the confirmation dialog box, to update the FortiAP to the selected firmware version.

FortiAP clients

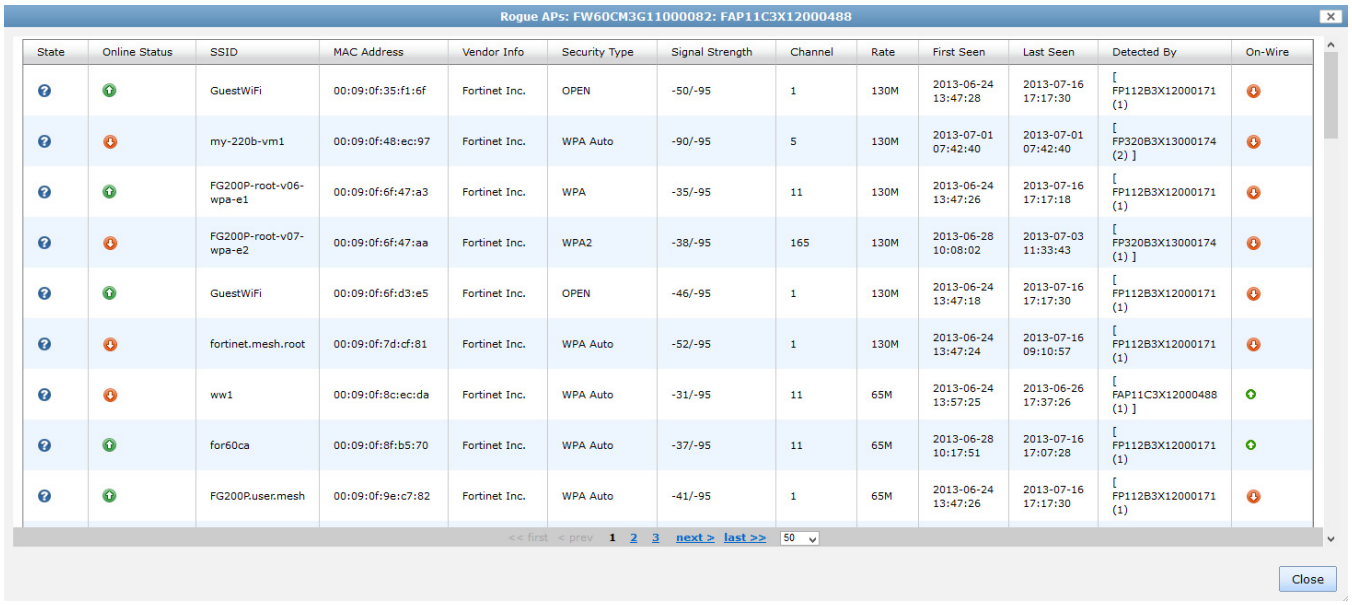
To view the FortiAP client list, right-click on a device in the FortiAP list and select *View Clients* from the pop-up menu. The FortiAP client list dialog box opens, displaying the following information:

IP	The device IP address.
FortiAP	The device serial number.
SSID Name	The SSID name used by the device.
MAC Address	The device's MAC address.
Auth	The device's authentication.
Vendor Info	The device vendor information.
Rate	The transfer rate of the device.
Signal Strength	The signal strength provided by the device.
Idle Time	The amount of time the device has been idle.
Association Time	The time the device has been associated.
Bandwidth Tx/Rx	The available bandwidth.

Rogue APs

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

Figure 92: Rogue AP list



The following information is shown:

State	The state of the device, if known.
Online Status	The status of the device: whether or not it is online.
SSID	The SSID used by the device.
MAC Address	The device's MAC address.
Vendor Info	The device vendor information.
Security Type	The type of security used by the device.
Signal Strength	The signal strength of the device.
Channel	The channel being used by the device.
Rate	The rate of the device.
First Seen	The time the device was first seen.
Last Seen	The time the device was last seen.
Directed By	The device directing the rogue AP.
On-Wire	If the device is on-wire.
Page controls	Scroll through the various pages of rogue AP listings.

Working with device groups

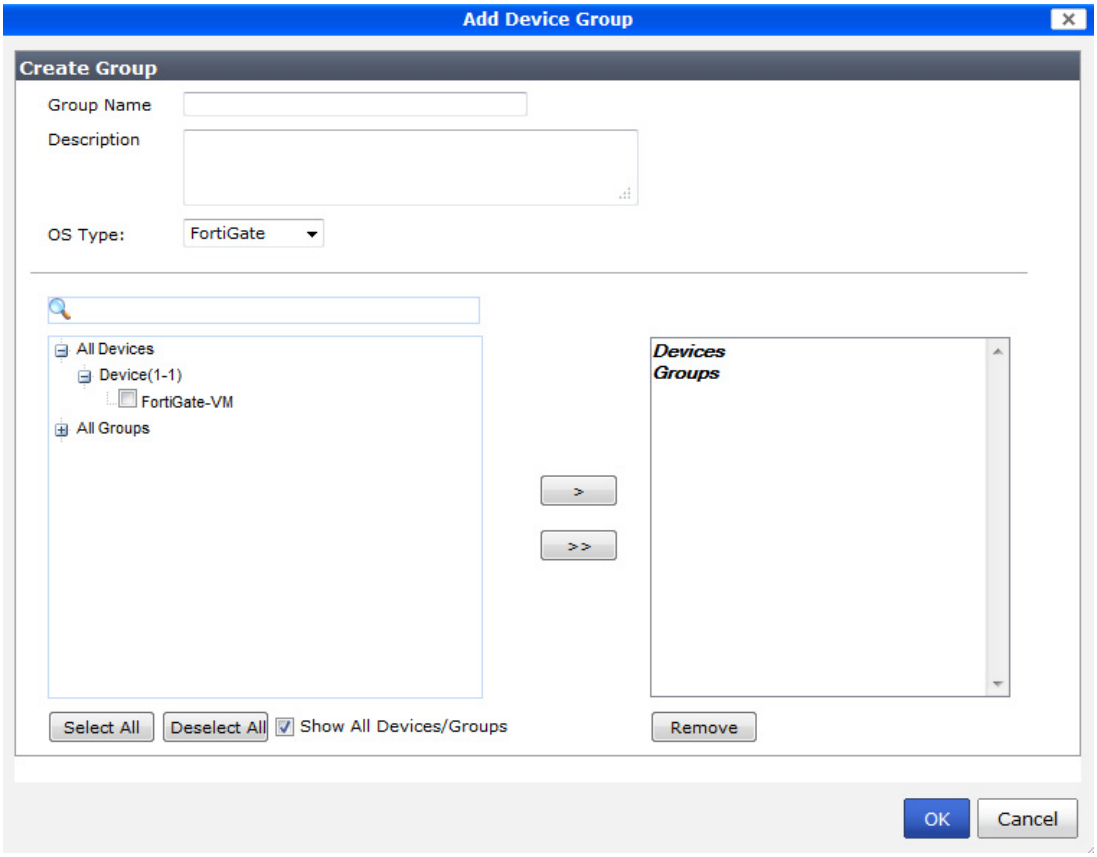
Device groups can be added, deleted, and edited as required to assist you in organized your managed devices.

To add a device group:

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

   The add *Device Group window* opens.

Figure 93: Adding a group



2. Complete the following fields:

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

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

3. Select *OK* to add the group.

To edit a device group:

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

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

To delete a device group

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



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

Managing FortiGate chassis devices

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



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

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

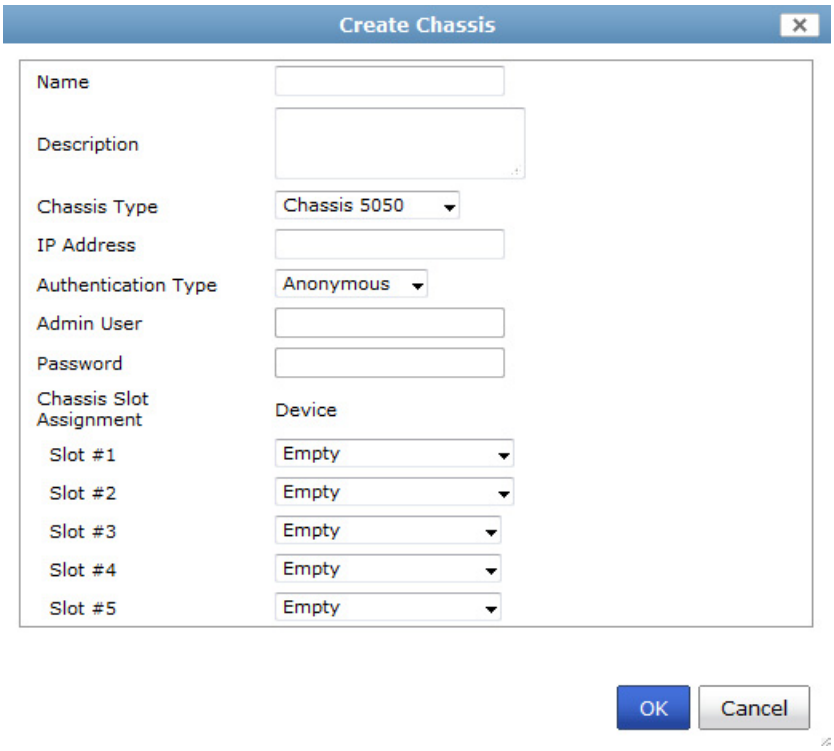
To enable chassis management:

1. In the *System Settings* tab, go to *System Settings* > *Advanced* > *Advanced Settings*. See “Advanced Settings” on page 127 for more information.
2. Under *Advanced Settings*, select *Chassis Management*.
3. Set the *Chassis Update Interval*; the value can be from 4 to 1440 minutes.

To add a chassis:

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

Figure 94: Add a new chassis



2. Complete the following fields:

Name	Enter a unique name for the chassis.
Description	Optionally, enter any comments or notes about this chassis.
Chassis Type	Select the chassis type: Chassis 5050, 5060, 5140 or 5140B.
IP Address	Enter the IP address of the Shelf Manager running on the chassis.
Authentication Type	Select Anonymous, MD5, or Password from the drop-down list.
Admin User	Enter the Admin user name.
Password	Enter the admin user password.
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 173.

3. Select *OK*.

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

1. In the Device Manager tab, right-click the chassis you want to edit and select *Edit* from the pop-up menu.
2. Modify the fields except *Chassis Type*, as required.
3. For *Chassis Slot Assignment*, from the drop-down list of a slot, select a FortiGate-5000 series blade to assign it to the slot. You can select a FortiGate, FortiCarrier, or FortiSwitch unit.



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

4. Select *OK*.

Viewing chassis dashboard

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

Viewing the status of the FortiGate blades

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

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

Current Sensors	Indicates if the current sensors for the blade in each slot are detecting a current within an acceptable range. *OK* indicates that all monitored currents are within acceptable ranges. *Critical* indicates that a monitored current is too high or too low.
Voltage Sensors	Indicates if the voltage sensors for the blade in each slot are detecting a voltage within an acceptable range. *OK* indicates that all monitored voltages are within acceptable ranges. *Critical* indicates that a monitored voltage is too high or too low.
Power Allocated	Indicates the amount of power allocated to each blade in the slot.
Action	Select *Activate* to turn the state of a blade from *Installed* into *Running*. Select *Deactivate* to turn the state of a blade from *Running* into *Installed*.
Edit 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 174.
Browse icon	Select to update the slot.

To edit voltage and temperature values:

1. Go to *[chassis name]* > *Blades* and, in the content pane, select the *Edit* icon of a slot.

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

   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.
3. Select *OK*.

Viewing the status of the power entry modules

You can view the status of the PEMs by going to *[chassis name]* > *PEM*.

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

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

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

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

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

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

Viewing shelf manager status

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

Refresh	Select to update the current page.
Shelf Manager	The order numbers of the shelf managers in the chassis.
Model	The shelf manager model.
State	The operation status of the shelf manager.
Temperature	The temperature of the shelf manager.
-48V Bus A	Status of the -48V Bus A: present or absent.
-48V Bus B	Status of the -48V Bus B: present or absent.
Power Allocated	Power allocated to each shelf manager.

Voltage Sensors	Lists the voltage sensors for the shelf manager.
State	Indicates if the voltage sensors for the shelf manager are detecting a voltage within an acceptable range. *OK* indicates that all monitored voltages are within acceptable ranges. *Below lower critical* indicates that a monitored voltage is too low.
Voltage	Voltage value for a voltage sensor.
Edit 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.

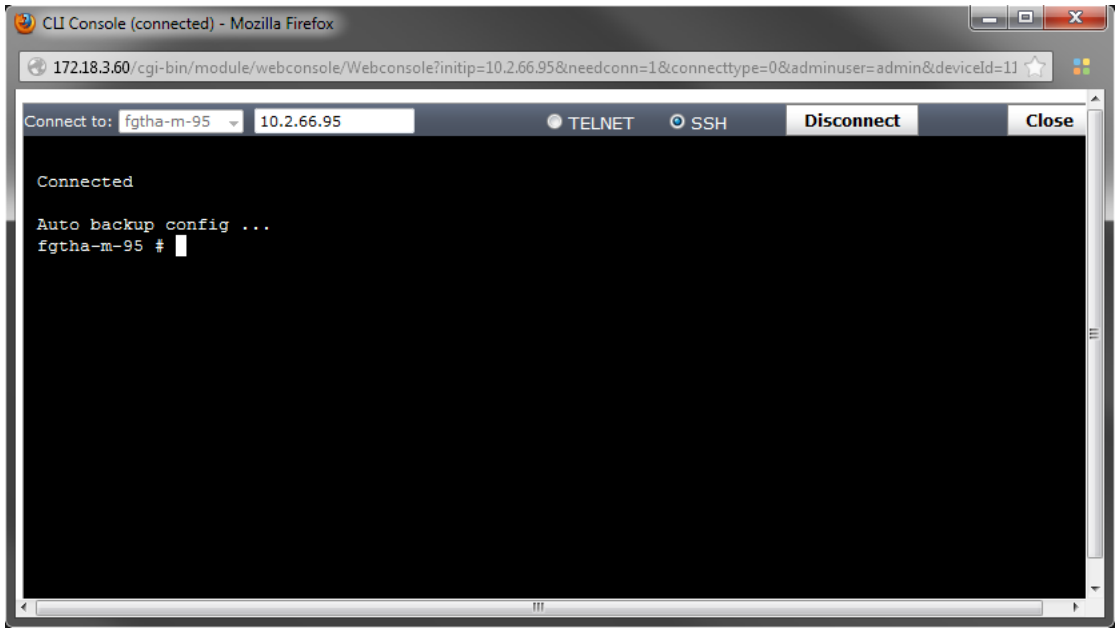
Go to *[chassis name]* > *SAP* to view the chassis SAP status.

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

Using the CLI console for managed devices

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

Figure 95:CLI console



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

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

Provisioning Templates

The provisioning templates section of the tree menu provides configuration options for System Templates, WiFi Templates, Endpoint Templates, and Certificate Templates.

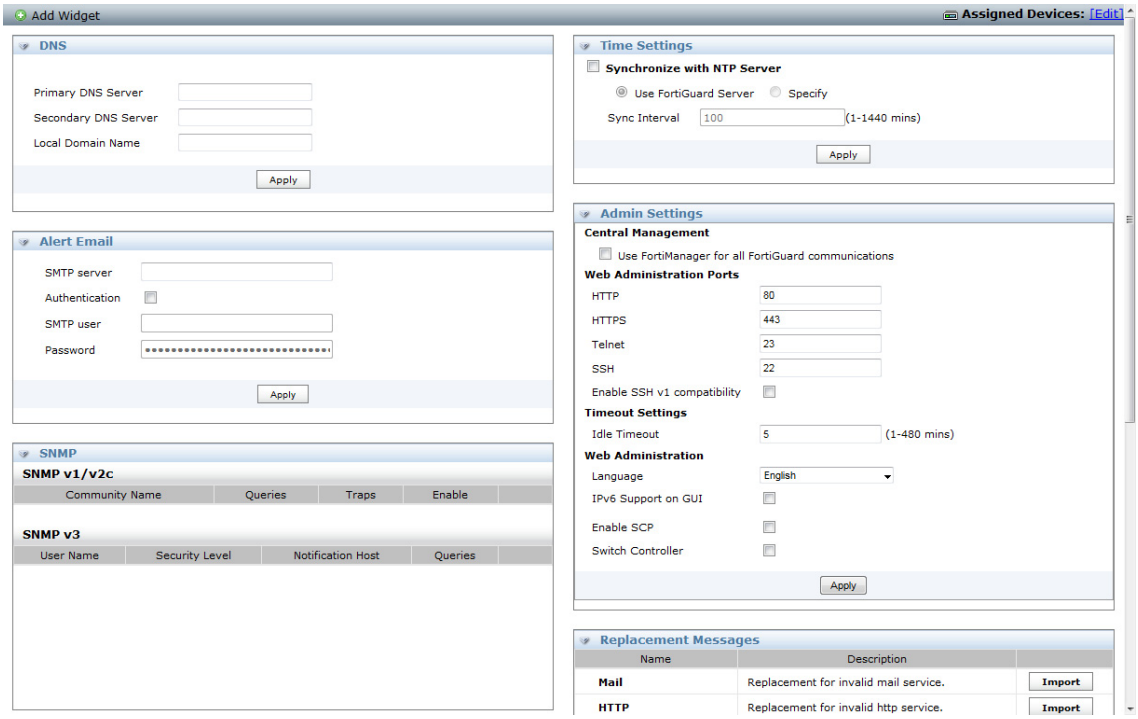
System Templates

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

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

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

Figure 96: System Templates



The following widgets and settings are available:

Widget	Description
DNS	Primary DNS Server, Secondary DNS Server, and Local Domain Name settings. Configure in the system template or import settings from a specific device.
Time Settings	Synchronize with NTP Server and Sync Interval settings. Configure in the system template or import settings from a specific device.
Alert Email	SMTP Server settings. Configure in the system template or import settings from a specific device.
Admin Settings	Web Administration Ports, Timeout Settings, and Web Administration. Configure in the system template.
SNMP	SNMP v1/v2 and SNMP v3 settings. Configure in the system template.

Replacement Messages	Global only, you can customize per VDOM replacement messages. Configure in the system template.
Log Settings	Send Logs to FortiAnalyzer/FortiManager (This FortiManager, Specify IP, Managed FortiAnalyzer) and Syslog settings. Configure in the system template.
FortiGuard	Enable FortiGuard Security Updates. Configure in the system template.

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

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

WiFi Templates

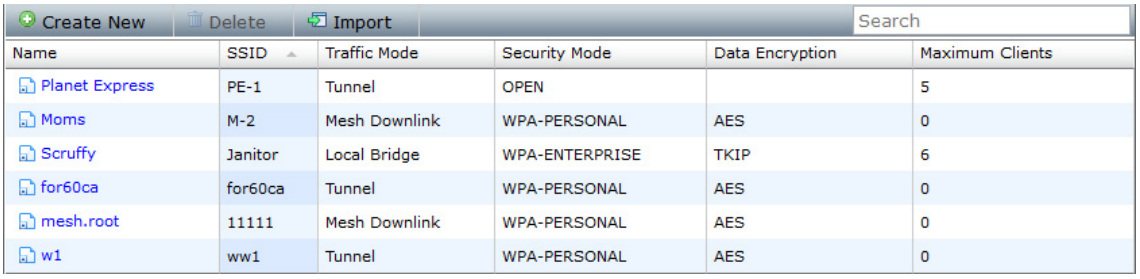
The WiFi Templates menu allows you to create and manage SSIDs, Wireless Profiles, and WIDS Profiles that can be applied to managed FortiAP devices.

SSIDs

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

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

Figure 97:SSIDs list



The following information is available:

Create New	Create a new SSID. See "To create a new SSID:" on page 180.
Delete	Select to delete the selected SSIDs. See "To delete an SSID or SSIDs:" on page 184.
Import	Select to import SSIDs. See "To import an SSID:" on page 185.
Search	Search the SSIDs by entering a search term in the search field.

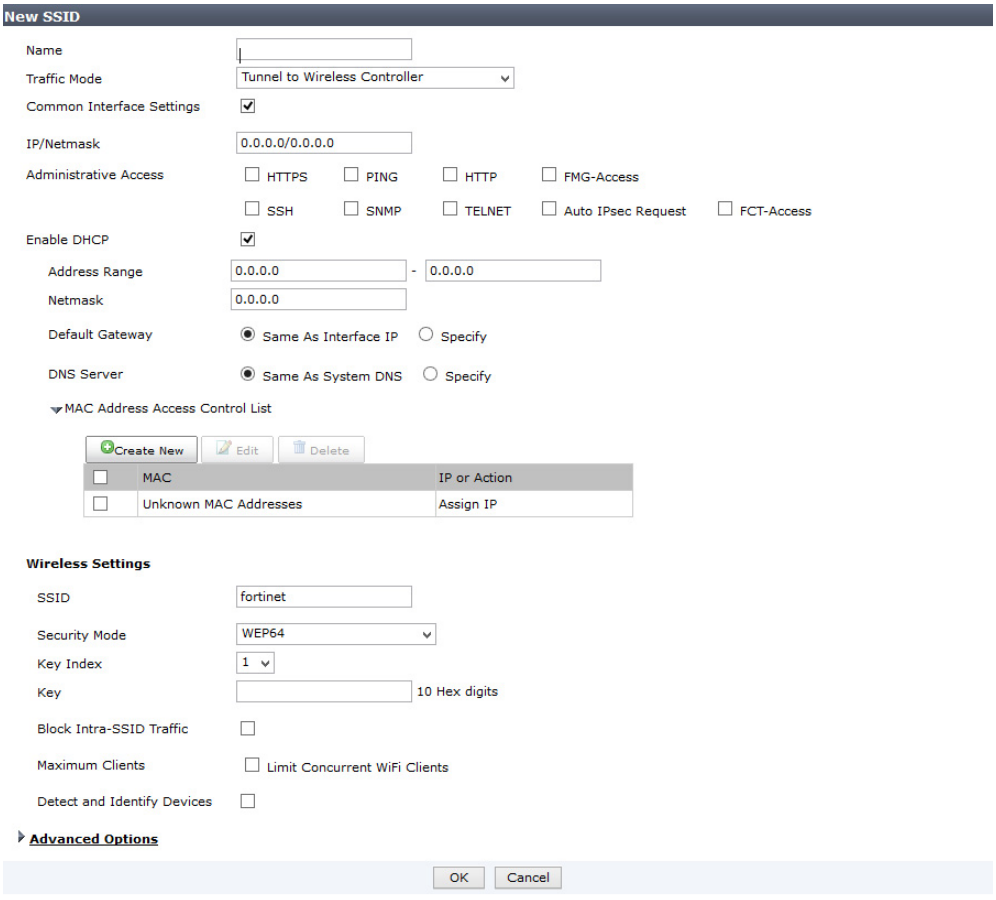
Name	The name given to the SSID.
SSID	The SSID name that is broadcast.
Traffic Mode	The traffic mode for the SSID; one of: *Tunnel to Wireless Controller*, *Local bridge with FortiAP's Interface*, or *Mesh Downlink*.
Security Mode	The security mode for the SSID; one of: *WPA-Personal*, *WPA-Enterprise*, *Captive Portal*, or *OPEN*.
Data Encryption	The data encryption method for the SSID.
Maximum Client	The maximum number of clients that can connect to the SSID at one time.

To create a new SSID:

1. From the SSIDs page, select *Create New*.

   The *New SSID* window opens.

Figure 98: New SSID



2. Enter the following information:

Name	Enter a name for the SSID.
Traffic Mode	Select the traffic mode from the drop-down list. The available options are: *Tunnel to Wireless Controller*, *Local bridge with FortiAP's Interface*, and *Mesh Downlink*.

Common Interface Settings	Select to enable common interface settings. Only available when Traffic Mode is set to *Tunnel to Wireless Controller*.
IP/Netmask	Enter the IP address and netmask. Only available when Traffic Mode is set to *Tunnel to Wireless Controller*.
Administrative Access	Select the allowed administrative service protocols from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, FMG-Access, Auto IPsec Request, and FCT-Access. Only available when Traffic Mode is set to *Tunnel to Wireless Controller*.
Enable DHCP	Select to enable and configure DHCP. Only available when Traffic Mode is set to *Tunnel to Wireless Controller*.
Address Range	Enter the DHCP address range.
Netmask	Enter the netmask.
Default Gateway	Select *Same As Interface IP* if the default gateway is the same as the interface IP's, or select *Specify* and enter a new gateway.
DNS Server	Select *Same As System DNS* if the DNS server is the same as the system DNS's, or select *Specify* and enter a DNS server address.
MAC Address Access Control List	The MAC address control list allows you to view the MAC addresses and their actions. It includes a default entry for unknown MAC addresses. Select *Create New* to create a new IP MAC binding. Select an address and then select *Edit* to edit the default action for unknown MAC addresses or your IP MAC bindings. Select an address or addresses and then select *Delete* to delete the selected items. The unknown MAC address cannot be deleted.
Wireless Settings	
SSID	Enter the wireless service set identifier (SSID) or network name for this wireless interface. Users who want to use the wireless network must configure their computers with this network name.

Security Mode	Select a security mode. The options are: *WEP64, WEP128, WPA/WPA2-PERSONAL*, *WPA/WPA2-ENTERPRISE, Captive Portal*, *OPEN*, *WPA-ONLY-PERSONAL, WAP-ONLY-ENTERPRISE, WPA2-ONLY-PERSONAL,* or *WPA2-ONLY-ENTERPRISE*. *Captive Portal* is not available if the traffic mode is set to *Mesh Downlink*. When *Traffic Mode* is set to *Mesh Downlink*, the security mode options are: *WPA/WPA2-PERSONAL, OPEN, WPA-ONLY-PERSONAL,* or *WPA2-ONLY-PERSONAL.*
Key Index	Select 1, 2, 3, or 4 from the drop-down menu. Many wireless clients can configure up to four WEP keys. Select which key clients must use.with this access point. This is available when `security` is a WEP type. This option is only available when Traffic Mode is set to *Tunnel to Wireless Controller* or *Local bridge with FortiAP's Interface*.
Key	Enter 10 Hex digits for the key value. This option is only available when Traffic Mode is set to *Tunnel to Wireless Controller* or *Local bridge with FortiAP's Interface*.
Data Encryption	Select the data encryption method. The options are: *AES*, *TKIP*, and *TKIP-AES*. This option is only available when the security mode is set to WPA.
Pre-shared Key	Enter the pre-shared key for the SSID. This option is only available when the security mode is set to *WPA-Personal*.
Detect and Identify Devices	Select to enable or disable detect and identify devices. When this setting is configured as enable, you can select to *Add New Devices to Vulnerability Scan List*.
Authentication	Select the authentication method for the SSID, either a RADIUS server or a usergroup, then select the requisite server or group from the respective drop-down list. This option is only available when the security mode is set to *WPA-Enterprise*.
Customize Portal Messages	Select to allow for customized portal messages. This option is only available when the security mode is set to *Captive Portal*.
User Groups	Select the user groups to add from the *Available* user group box. Use the arrow buttons to move the desired user groups to the *Selected* user groups box. This option is only available when the security mode is set to *Captive Portal*.

Block Intra-SSID Traffic	Select to block intra-SSID traffic. This option is only available when Traffic Mode is set to *Tunnel to Wireless Controller*.
Maximum Clients	Select to limit the concurrent WiFi clients that can connect to the SSID. If selected, enter the desired maximum number of clients. Enter 0 for no limit. This option is only available when Traffic Mode is set to *Tunnel to Wireless Controller* or *Local bridge with FortiAP's Interface*.
Advanced Options	Configure advanced options for the SSID.
broadcast-ssid	Enable broadcast of the SSID. Broadcasting the SSID enables clients to connect to your wireless network without first knowing the SSID. For better security, do not broadcast the SSID.
broadcast-suppression	Prevent ARP or DHCP messages being carried to other access points carrying the same SSID. Select DHCP and/or ARP broadcast suppression.
dynamic-vlan	Enable dynamic VLAN assignment for users based RADIUS attribute.
external-fast-roaming	Enable or disable pre-authentication with external non-managed APs.
fast-roaming	Select to enable or disable fast roaming. Enabling fast-roaming enables pre-authentication where supported by clients.
gtk-rekey-intv	Set the WPA re-key interval. Some clients may require a longer interval. Range 60 to 864 000 seconds.
local-authentication	Enable authentication of clients by the FortiAP unit if the wireless controller is unavailable. This applies only if `security` is a WPA-Personal mode and `local-bridging` is enabled.
local-switching	Enable or disable bridging of local VAP interfaces.
me-disable-thresh	Set the multicast enhancement threshold. Enter the threshold value in the text field.
multicast-enhance	Select to enable or disable multicast enhance.
portal-message-override-group	Select the portal message override group from the drop-down menu.
ptk-rekey-intv	Enter the rekey interval value in the text field.
radius-mac-auth	Select to enable or disable RADIUS MAC authentication.
radius-mac-auth-server	Select the RADIUS MAC authentication server from the drop-down list.

vlan-auto	Select to enable or disable automatic VLAN assignment for authenticated users of this SSID.
vlanid	Enter the VLAN ID in the text field. Enter 0 is VLANs are not used.

3. Select *OK* to create the new SSID.

To edit an SSID:

1. From the SSIDs page, double click on an SSID name or right-click on the name and select *Edit* from the pop-up menu.

   The *Edit SSID* window opens.
2. Edit the settings as required. The SSID name cannot be edited.
3. Selected *OK* to apply your changes.

To delete an SSID or SSIDs:

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

To clone an SSID:

1. From the SSIDs page, right-click on the SSID name and select *Clone* from the pop-up menu.

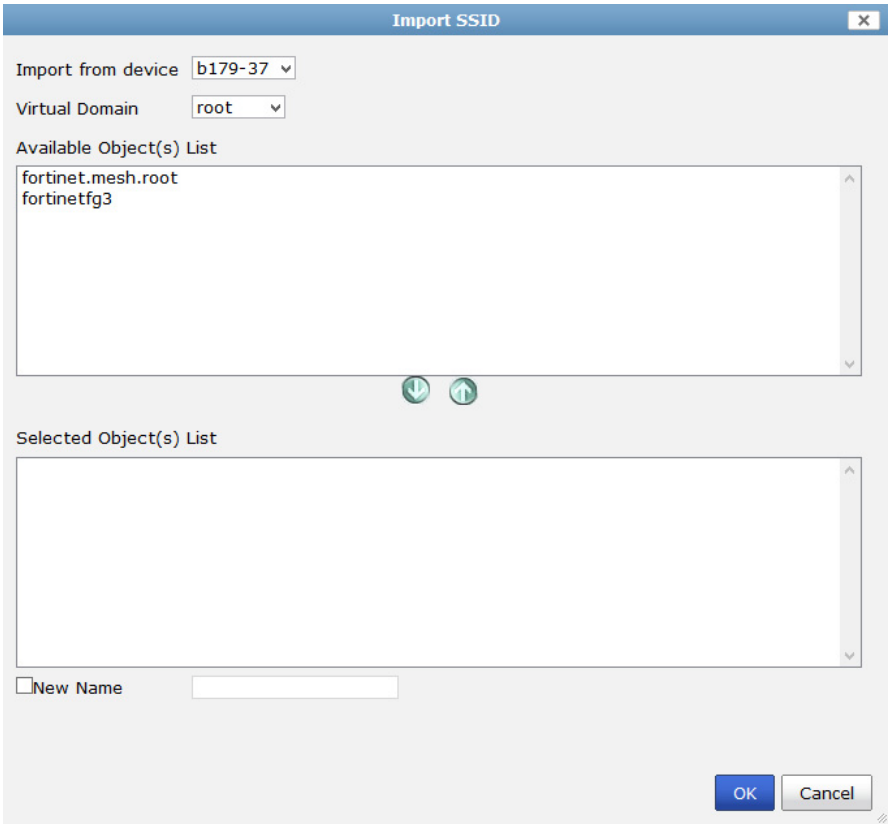
   The *Clone SSID* window opens.
2. Edit the settings as required.
3. Selected *OK* to clone the SSID.

To import an SSID:

1. From the SSIDs page, select *Import*.

   The *Import SSID* dialog box opens.

Figure 99: Import SSID



2. Enter the following information:

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

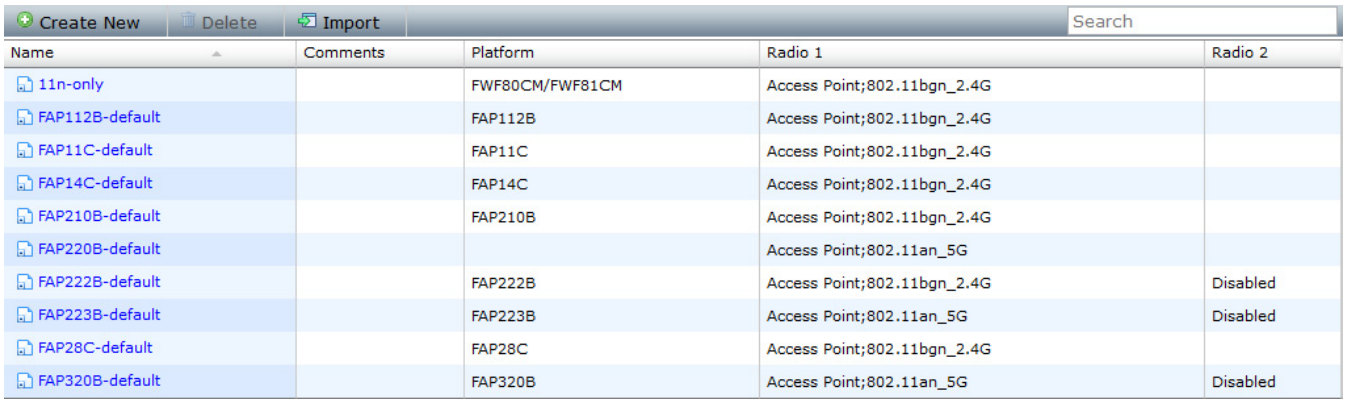
3. Select *OK* to import the SSID or SSIDs.

Wireless Profiles

The wireless profiles menu lists all of the wireless profiles available in the ADOM. Profiles can be created, edited, cloned, deleted, imported, and searched.

To view the wireless profiles, in the *Provisioning Profiles* tree menu, select an ADOM, then select *Wifi Templates> Wireless Profiles*.

Figure 100: Wireless profiles



The following information is available:

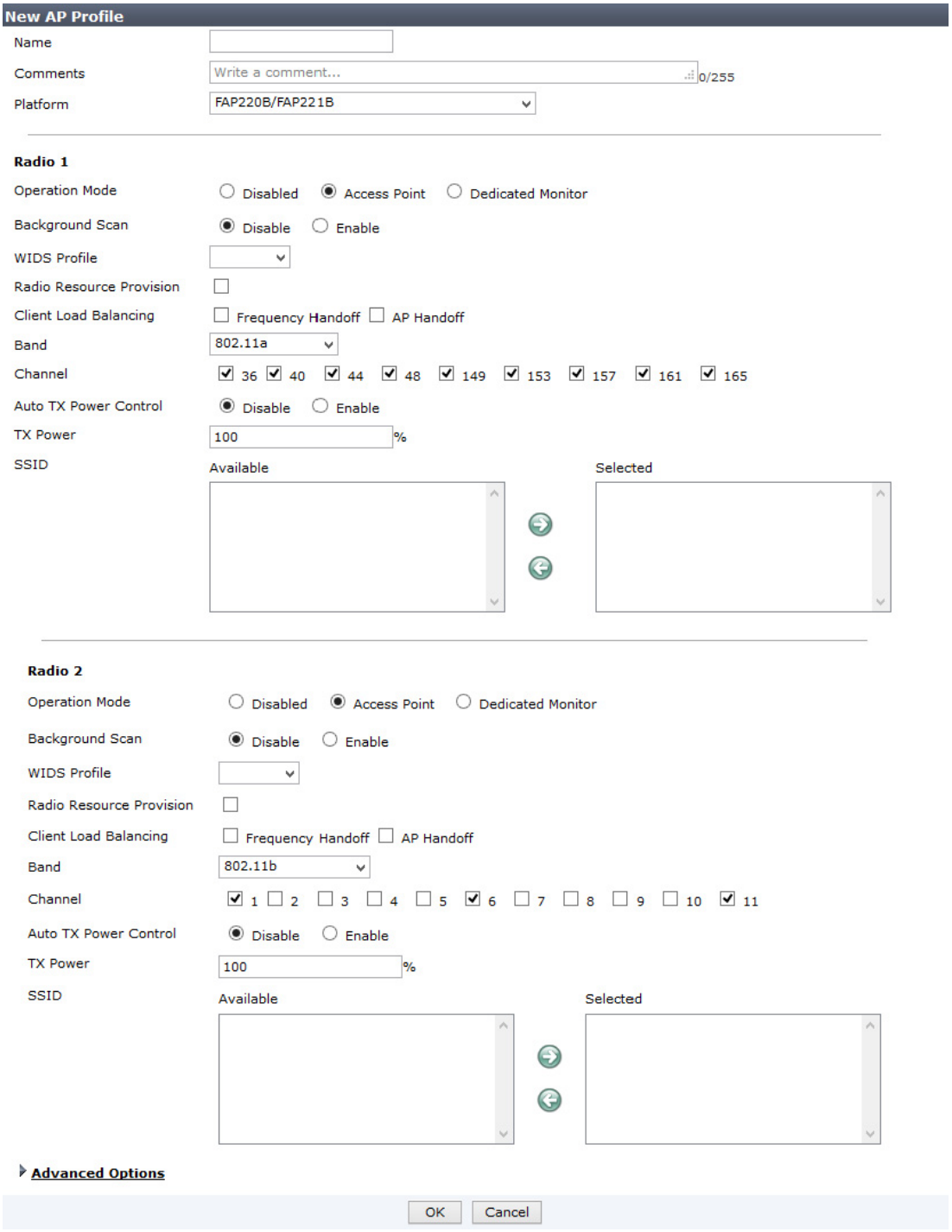
Create New	Create a new wireless profile. See “To create a new wireless profile:” on page 187.
Delete	Select to delete the selected wireless profiles. See “To delete a wireless profile:” on page 189.
Import	Select to import wireless profiles. See “To import a wireless profile:” on page 189.
Search	Search the wireless profiles by entering a search term in the search field.
Name	The profile’s name.
Comments	Comments about the profile.
Platform	The platform that the wireless profile applies to.
Radio 1	The function of the Radio 1 in the profile.
Radio 2	If applicable, the Radio 2 function in the profile.

To create a new wireless profile:

1. From the wireless profiles page, select *Create New*.

   The *New AP Profile* window opens.

Figure 101: New AP profile



2. Enter the following information:

Name	Enter a name for the profile.
Comment	Optionally, enter comments.

Platform	Select the platform that the profile will apply to from the drop-down list.
Radio 1 & 2	Configure the radio settings. The Radio 2 settings will only appear if applicable to the platform that is selected.
Operation Mode	Select one of *Disabled*, *Access Point* (default), or *Dedicated Monitor*. If *Disabled* is selected, no further options are available. If *Dedicated Monitor* is selected, only the WIDS profile and Rogue AP On-Wire Scan options are available.
Background Scan	Enable or disable background scanning.
WIDS Profile	Select a WIDS profile from the drop-down list.
Rogue AP On-Wire Scan	Select to enable rogue AP on-wire scan. This option is only available is the operation mode is set to *Dedicated Monitor*, or if background scan is enabled.
Radio Resource Provision	Select to enable radio resource provisioning.
Client Load Balance	Select the client load balancing methods to use. Frequency and/or AP handoff can be used.
Band	Selected the wireless band from the drop-down list. The bands available are dependent on the platform selected.
Channel	Select the channel or channels that are available. The channels available are dependent on the platform selected.
Auto TX Power Control	Enable or disable automatic TX power control.
TX Power	If *Auto TX Power Control* is disabled, enter the TX power in the form of the percentage of the total available power.
TX Power Low	If *Auto TX Power Control* is enabled, enter the minimum TX power in dBm.
TX Power High	If *Auto TX Power Control* is enabled, enter the maximum TX power in dBm.
SSID	Select available SSIDs from the *Available* box, and move them to the *Selected* box using the arrow buttons to select the SSIDs to apply to this profile.
Advanced Options	Configure advanced options for the SSID.
dtls-policy	Select clear-text, dtls-enable, or both.
handoff-rssi	Enter a value for RSSI handoff.

handoff-sta-thresh	Enter a value for the threshold.
max-clients	Enter a value for the maximum number of clients.

3. Select *OK* to create the new wireless profile.

To edit a wireless profile:

1. From the wireless profiles page, double click on a wireless profile's name or right-click on the name and select *Edit* from the pop-up menu.

   The *Edit AP Profile* window opens.
2. Edit the settings as required. The profile name cannot be edited.
3. Selected *OK* to apply your changes.

To delete a wireless profile:

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

To clone a wireless profile:

1. From the wireless profiles page, right-click on a profile name and select *Clone* from the pop-up menu.

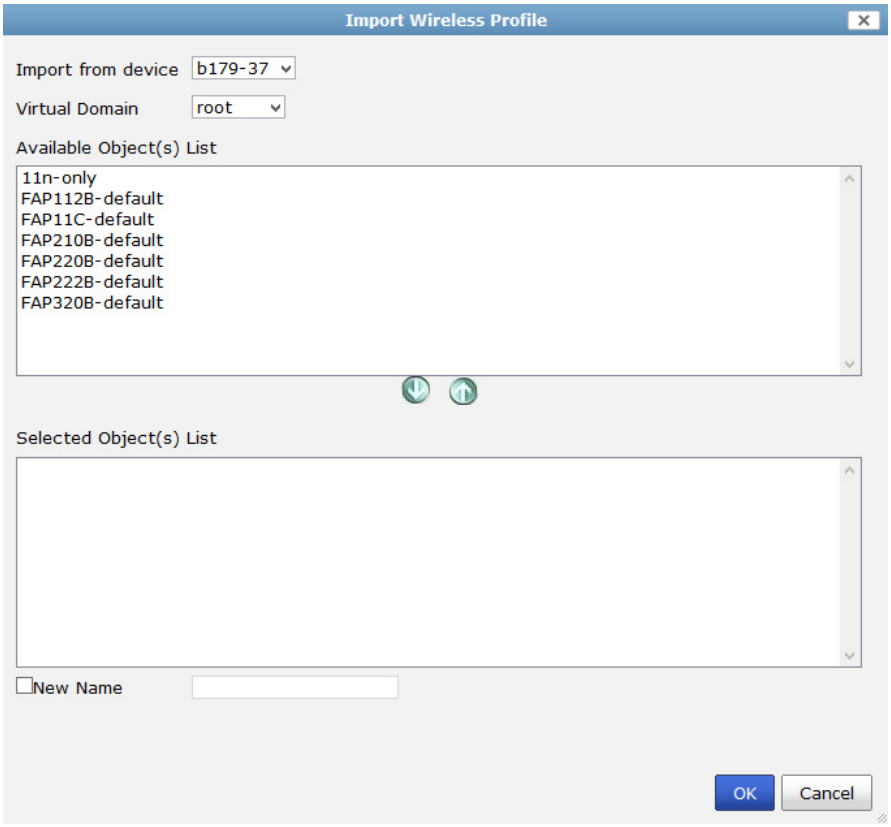
   The *Edit AP Profile* window opens.
2. Edit the name of the profile, then edit the remaining settings as required.
3. Selected *OK* to clone the profile.

To import a wireless profile:

1. From the wireless profile page, select *Import*.

   The *Import Wireless Profile* dialog box opens.

Figure 102: Import wireless profile



2. Enter the following information:

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

3. Select *OK* to import the profile or profiles.

WIDS Profile

The WIDS monitors wireless traffic for a wide range of security threats by detecting and reporting on possible intrusion attempts. When an attack is detected, a log message is recorded.

WIDS profiles can be created, edited, cloned, deleted, imported, and searched. A default profile is available by default.

To view the wireless profiles, in the *Provisioning Profiles* tree menu, select an ADOM, then select *Wireless Profiles* > *WIDS Profiles*. The WIDS profile list is displayed, with the following information is available:

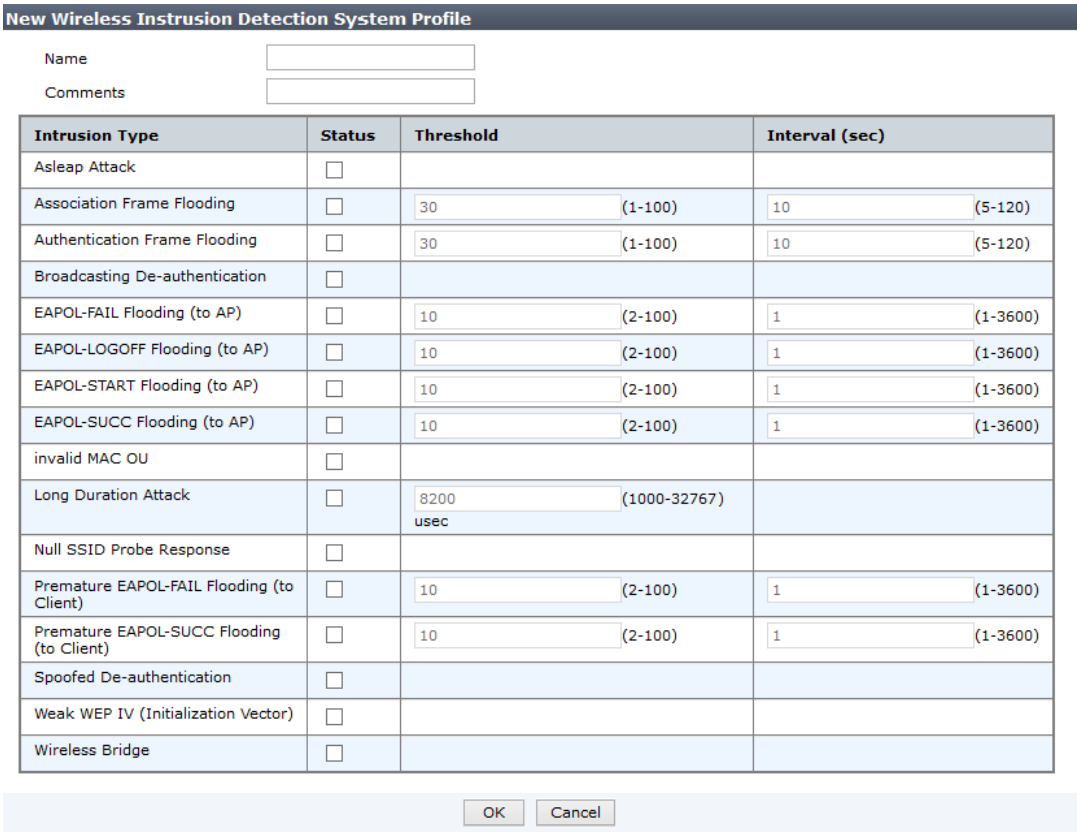
Create New	Create a new WIDS profile. See “To create a new WIDS profile:” on page 192.
Delete	Select to delete the selected WIDS profiles. See “To delete a WIDS profile:” on page 194.
Import	Select to import WIDS profiles. See “To import a WIDS profile:” on page 194.
Search	Search the WIDS profiles by entering a search term in the search field.
Name	The profile’s name.
Comments	Comments about the profile.

To create a new WIDS profile:

1. From the WIDS profiles page, select *Create New*.

   The *New Wireless Intrusion Detection System Profile* window opens.

Figure 103: New WIDS profile



2. Enter the following information:

Name	Enter a name for the profile.
Comment	Optionally, enter comments.
Intrusion Type	The intrusion types that can be detected. See Table 11 on page 193 for information on the available types.
Status	Select the status of the intrusion type (enable it).
Threshold	If applicable, enter a threshold for reporting the intrusion.
Interval (sec)	If applicable, enter the interval for reporting the intrusion, in seconds.

3. Select *OK* to create the new wireless profile.

Table 11 provides a list of intrusion types and the description.

Table 11: Intrusion types

Intrusion Type	Description
Asleap Attack	ASLEAP is a tool used to perform attacks against LEAP authentication.
Association Frame Flooding	A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
Authentication Frame Flooding	A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
Broadcasting De-authentication	This is a type of Denial of Service attack. A flood of spoofed de-authentication frames forces wireless clients to de-authenticate, then re-authenticate with their AP.
EAPOL Packet Flooding (to AP)	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the AP with these packets can be a denial of service attack. Several types of EAPOL packets can be detected: EAPOL-FAIL, EAPOL-LOGOFF, EAPOL-START, and EAPOL-SUCC.
Invalid MAC OU	Some attackers use randomly-generated MAC addresses. The first three bytes of the MAC address are the Organizationally Unique Identifier (OUI), administered by IEEE. Invalid OUIs are logged.
Long Duration Attack	To share radio bandwidth, WiFi devices reserve channels for brief periods of time. Excessively long reservation periods can be used as a denial of service attack. You can set a threshold between 1000 and 32 767 microseconds. The default is 8200.
Null SSID Probe Response	When a wireless client sends out a probe request, the attacker sends a response with a null SSID. This causes many wireless cards and devices to stop responding.
EAPOL Packet Flooding (to client)	Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the client with these packets can be a denial of service attack. Two types of EAPOL packets can be detected: EAPOL-FAIL, and EAPOL-SUCC.
Spoofed De-authentication	Spoofed de-authentication frames form the basis for most denial of service attacks.
Weak WEP IV Detection	A primary means of cracking WEP keys is by capturing 802.11 frames over an extended period of time and searching for patterns of WEP initialization vectors (IVs) that are known to be weak. WIDS detects known weak WEP IVs in on-air traffic.
Wireless Bridge	WiFi frames with both the FromDS and ToDS fields set indicate a wireless bridge. This will also detect a wireless bridge that you intentionally configured in your network.

To edit a WIDS profile:

1. From the WIDS profiles page, double click on a profile's name or right-click on the name and select *Edit* from the pop-up menu.

   The *Edit Wireless Intrusion Detection System Profile* window opens.
2. Edit the settings as required.
3. Selected *OK* to apply your changes.

To delete a WIDS profile:

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

To clone a WIDS profile:

1. From the WIDS profiles page, right-click on a profile name and select *Clone* from the pop-up menu.

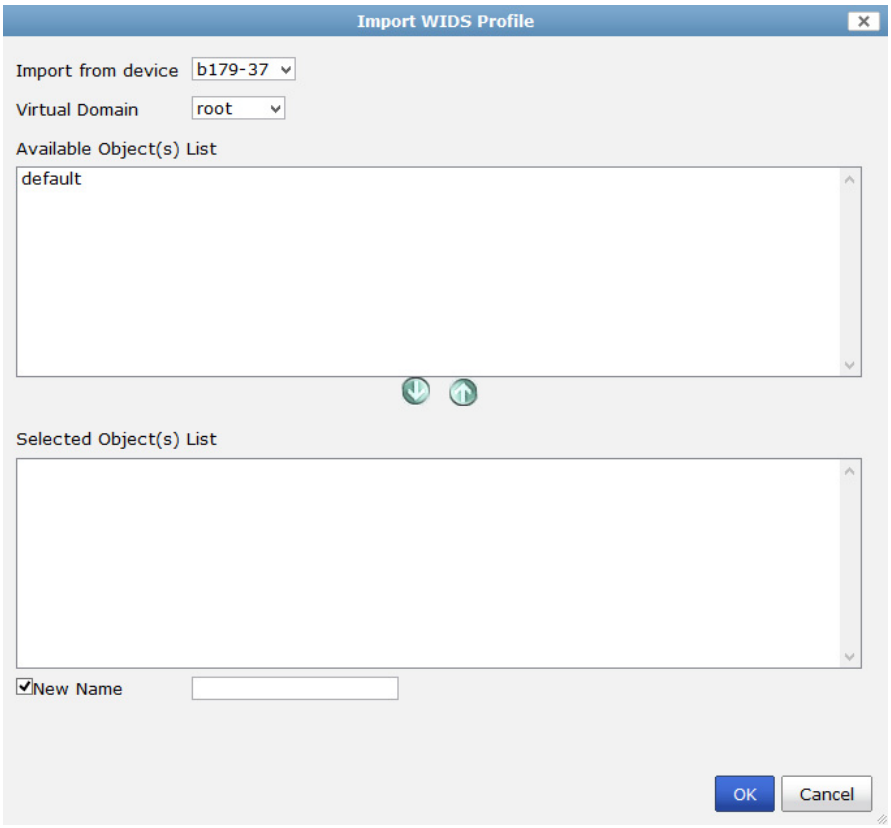
   The *Edit Wireless Intrusion Detection System Profile* window opens.
2. Edit the name of the profile, then edit the remaining settings as required.
3. Selected *OK* to clone the profile.

To import a WIDS profile:

1. From the WIDS profile page, select *Import*.

   The *Import WIDS Profile* dialog box opens.

Figure 104: Import WIDS profile



2. Enter the following information:

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

3. Select *OK* to import the profile or profiles.

Endpoint Templates

The endpoint templates menu allows you to create and manage endpoint and client reputation profiles, which can then be assigned to devices.

Endpoint control ensures that workstation computers (endpoints) meet security requirements, otherwise they are not permitted access. Endpoint Control enforces the use of FortiClient Endpoint Security and pushes an Endpoint Profile to the FortiClient application.

The endpoint profile consists of the following sections:

- Antivirus Realtime Protection on Client
- Application Firewall

  You can select the application control sensor to associate with the endpoint profile.
- Web Category Filtering

  You can select the web filtering profile to associate with the endpoint profile. You can also select to disable Web Category Filtering when the client is protected by the FortiGate.
- Endpoint Vulnerability on Client

  You can select to scan daily, weekly or monthly. You can also select to scan the client after registration with your FortiGate device.
- Client VPN Provisioning

  You can specify the VPN name, type, gateway and other settings the client will use to connect to your FortiGate device via the VPN connection. Two-factor authentication is configured in the FortiGate VPN configuration.
- Upload logs to FortiAnalyzer/FortiManager

  You can select to use the same IP address as the FortiGate device or specify a different device IP address. You can specify the frequency of the log upload.

- Use FortiManager for client software/signature update

  Select to enable this feature and enter the IP address of your FortiManager device. You can select to failover over to the FortiGuard Distribution Network (FDN) when the FortiManager is not available.

- Advanced options

  You can customize which modules are displayed in the FortiClient dashboard. This will allow you to activate any of the modules at a later date without needing to re-install FortiClient. Select to show/hide FortiClient modules in the client console. You can also select to hide banners.

  Select if profile details may be displayed before endpoint control registration is completed.

Non-compliant endpoints are those without the latest version of FortiClient installed. They can be sent to the FortiClient download portal to obtain FortiClient software, or they can be blocked. For more information on configuring Endpoint Profiles and Endpoint Control, see the *FortiClient Administration Guide*.

Endpoint Profiles

When an endpoint profile is selected in a firewall policy, all users of that firewall policy must have FortiClient Endpoint Security installed. The endpoint profile settings are pushed to the FortiClient application on the client.

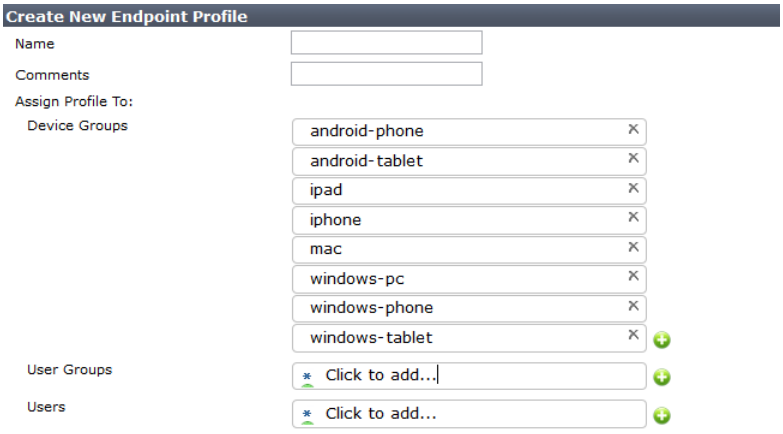
Endpoint profiles can be created, edited, cloned, deleted, and imported from devices using right-click menu and toolbar selections.

To create a new endpoint profile:

1. Go to the *Endpoint Templates* > *Endpoint Profile* page and select *Create New*.

   The *Create New Endpoint Profile* page opens.

   Figure 105: New endpoint profile



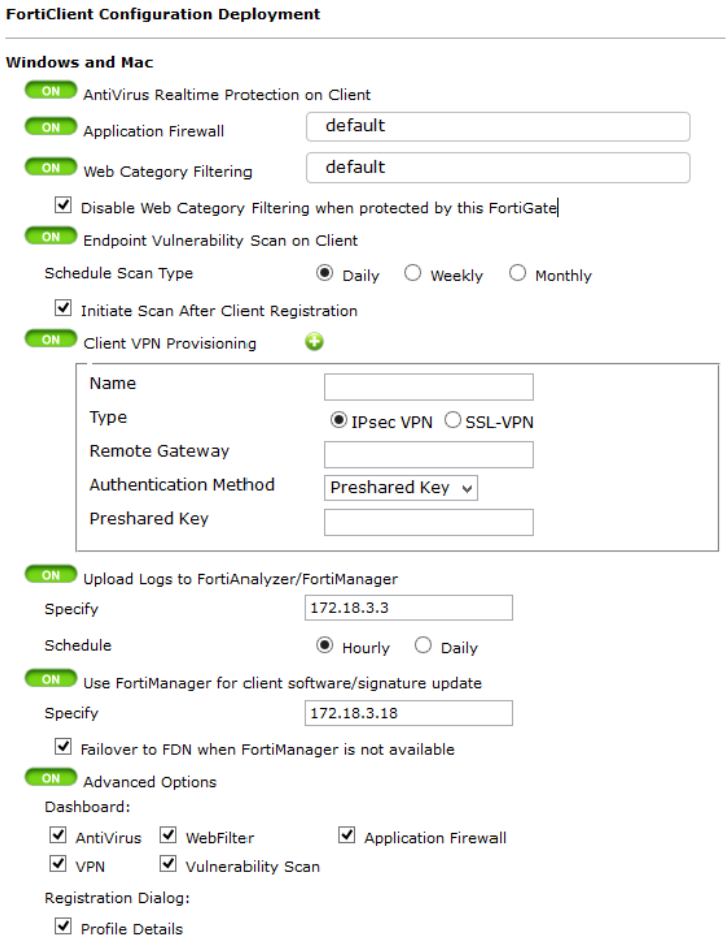
2. Enter the following information:

Name	Enter a name for the new endpoint profile. When creating a new endpoint profile, XSS vulnerability characters are not allowed.

Comments	Enter a profile description. (optional)
Assign to Profile To:	Device Groups: Select device groups in the drop-down menu. Use the plus (+) icon to assign multiple device groups to the endpoint profile, for example Mac and Windows PC. User Groups: Select user groups in the drop-down menu. Select the plus (+) icon to assign multiple user groups to the endpoint profile. Users: Select users in the drop-down menu. Select the plus (+) icon to assign multiple users to the endpoint profile. ***Note:*** You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN.

3. Continue down the page to the operating system specific settings.

Figure 106: FortiClient configuration deployment for Windows and Mac



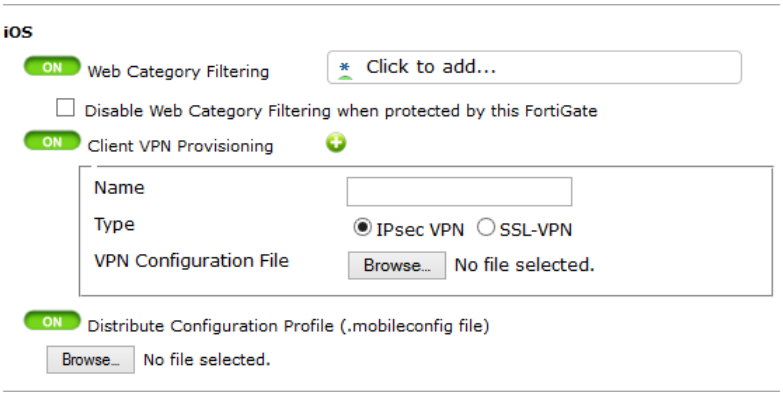
4. Enter the following information for the Windows and Mac section:

FortiClient Configuration Deployment ***Windows and Mac***	
Antivirus Realtime Protection on Client	Toggle the button on or off to enable or disable this feature.
Application Firewall	Toggle the button on or off to enable or disable this feature. When enabled, you can select an application control sensor in the drop-down menu.
Web Category Filtering	Toggle the button on or off to enable or disable this feature. When enabled, you can select a web filter profile in the drop-down menu. Select the checkbox to disable web category filtering on the client when protected by the FortiGate.
Endpoint Vulnerability Scan on Client	Toggle the button on or off to enable or disable this feature. When enabled, you can select the scheduled scan type to daily, weekly, or monthly. Select the checkbox to initiate a scan after client registration with the FortiGate.
Client VPN Provisioning	Toggle the button on or off to enable or disable this feature. When enabled, you can configure multiple IPsec VPN and SSL VPN connections. Select the plus (+) icon to add additional VPN connections. Enter the VPN name, type, remote gateway, and authentication method information.
Upload Logs to FortiAnalyzer/FortiManager	Toggle the button on or off to enable or disable this feature. When enabled, you can select to use the same FortiAnalyzer/FortiManager used by the FortiGate or select *Specify* to enter a different device IP. You can set the schedule to hourly or daily. The FortiClient upload logs to the FortiAnalyzer/FortiManager only when it is able to connect to the device on the specified IP address.

Use FortiManager for client software/signature update	Toggle the button on or off to enable or disable this feature. When enabled, you can specify the IP address of the FortiManager. Select the checkbox to failover to the FortiGuard Distribution Network when the FortiManager is not available.
Advanced Options	Toggle the button on or off to enable or disable these features. When enabled, you can select which FortiClient modules are visible in the FortiClient console window. Select the appropriate checkbox to show the module. You can also select to show profile details for the Registration dialog.

5. If required, enter the *FortiClient Configuration Deployment* settings for *iOS*.

Figure 107: FortiClient configuration deployment for iOS



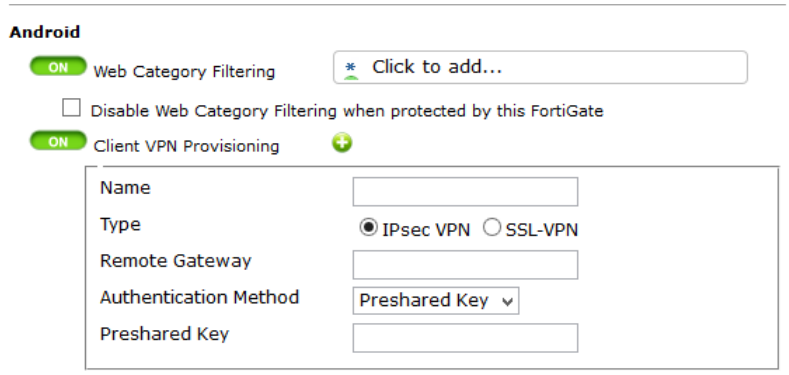
6. Configure the following settings:

Web Category Filtering	Toggle the button on or off to enable or disable this feature. When enabled, you can select a web filter profile in the drop-down menu. Select the checkbox to disable web category filtering on the client when protected by the FortiGate.
Client VPN Provisioning	Enable to configure the FortiClient VPN client. You can enter multiple VPN configurations by selecting the “+” button. Optionally, you can upload the FortiClient iOS VPN configuration file.
Name	Enter a name to identify this VPN configuration in the FortiClient application.

Type	Select *IPsec VPN* or *SSL-VPN*. If you select *IPsec VPN*, select a *VPN Configuration File* that contains the required IPsec VPN configuration. The Apple iPhone Configuration Utility/Apple Configurator produces `.mobileconfig` files which contain configuration information for an iOS device. If you select *SSL-VPN*, enter the VPN configuration details.
Distribute Configuration Profile	Distribute configuration information to iOS devices running FortiClient Endpoint Security. Select *Browse* and locate the file to be distributed. The Apple iPhone Configuration Utility/Apple Configurator produces `.mobileconfig` files which contain configuration information for an iOS device.

7. If required, enter the *FortiClient Configuration Deployment* settings for *Android*.

Figure 108: FortiClient configuration deployment for Android



8. Configure the following settings:

Web Category Filtering	Toggle the button on or off to enable or disable this feature. When enabled, you can select a web filter profile in the drop-down menu. Select the checkbox to disable web category filtering on the client when protected by the FortiGate. Note: FortiClient (Android) only supports FortiGuard Categories settings in the Web Filter Profile. Only Allow and Block actions are supported. All other settings will be ignored by FortiClient (Android).
Client VPN Provisioning	Enable to configure the FortiClient VPN client. You can enter multiple VPN configurations by selecting the “+” button.
Name	Enter a name to identify this VPN configuration in the FortiClient application.
Type	Select *IPsec VPN* or *SSL-VPN*.
Remote Gateway	Enter the remote gateway.

Authentication Method	Select the authentication method to use, either *Preshared Key* or *Certificate*. If *Preshared Key* is selected, enter the your preshared key. This option is only available if the type is *IPsec VPN*.
Require Certificate	Select to require a certificate. This option is only available if the type is *SSL-VPN*.
Access Port	Enter the access port number. This option is only available if the type is *SSL-VPN*.

9. Select OK.

To edit an endpoint profile:

1. Double-click on the profile name, or right-click in the profile row and select *Edit* from the pop-up menu.
2. Edit the settings as required in the *Edit Endpoint Profile* window, then select *OK* to apply the changes.

To delete an endpoint profile:

1. Right-click in the profile row and select *Delete* from the pop-up menu.
2. Select *OK* in the confirmation dialog box to delete the profile.

To clone an endpoint profile:

1. Right-click in the row of the profile that you are cloning and select *Clone* from the pop-up menu.
2. In the *Edit Endpoint Profile* window, change the name of the endpoint profile.
3. Adjust the remaining settings as required, then select *OK* to create the cloned profile.

To import an endpoint profile:

1. From the endpoint profile page, select *Import*.
2. Enter the following information in the *Import Endpoint Profile* dialog box:

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

3. Select *OK* to import the profile.

Client Reputation

User or client behavior can sometimes increase the risk of being attacked or becoming infected. For example, if one of your network clients receives email viruses on a daily basis while no other clients receive these attachments, extra measures may be required to protect that client, or a discussion with the user about this issue may be warranted.

Before you can decide on a course of action, you need to know the problem is occurring. Client reputation can provide this information by tracking client behavior and reporting on activities that you determine are risky or otherwise worth tracking.

Client reputation profiles can be created, edited, and assigned to devices. When creating a profile, the default threat level definitions are used; these can be changed later, see "To adjust client reputation profile threat level definitions:" on page 202. For more information on configuring Client Reputation profiles, see the *FortiOS 5.0 Handbook*.

To create a new client reputation profile:

1. Go to the *Endpoint Templates* > *Client Reputation Profile* page and select *Create New*.
2. In the *New Client Reputation Profile* window, enter a name for the profile.
3. Select *OK* to create the new client reputation profile.

To edit a client reputation profile:

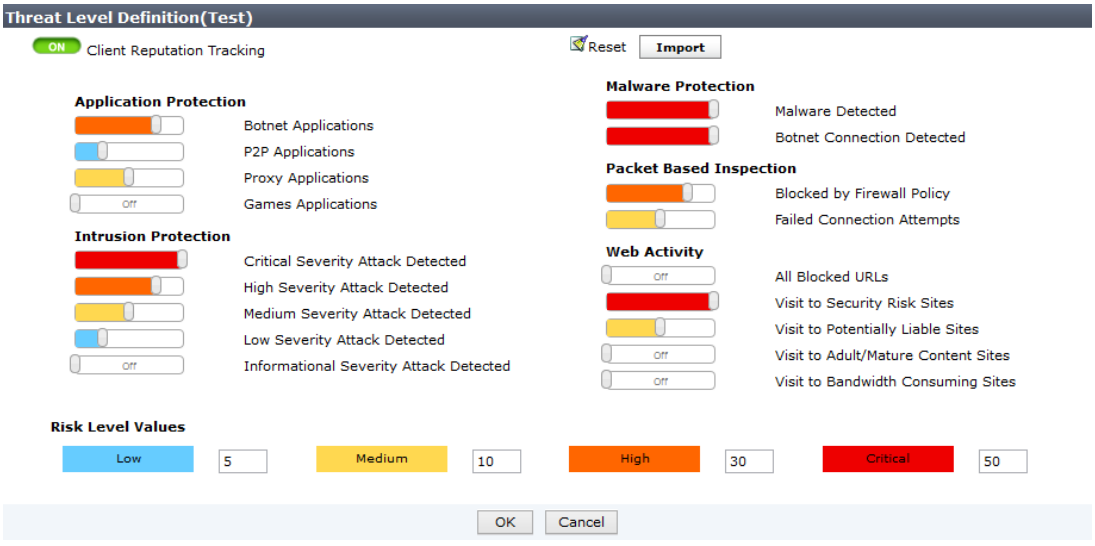
1. Right-click in the profile row and select *Edit* from the pop-up menu.
2. Edit the profile name as required, then select *OK*.

To adjust client reputation profile threat level definitions:

1. Click on a client reputation profile name.

   The *Threat Level Definition* page opens.

Figure 109: Threat level definitions



2. Adjust the threat levels as needed:

Client Reputation Tracking	Turn on client reputation tracking.
Reset	Reset all the threat level definition values back to their defaults.

Import	Import threat level definitions from a device in the ADOM.
Application Protection	Adjust the tracking levels for the different application types that can be tracked.
Intrusion Protection	Adjust the tracking levels for the different attack types that can be tracked.
Malware Protection	Adjust the tracking levels for the malware or botnet connections that can be detected.
Packet Based Inspection	Adjust the tracking levels for failed connection attempts and traffic blocked by firewall policies.
Web Activity	Adjust the tracking levels for various types of web activity.
Risk Level Values	Adjust the values for the four risk levels.

3. Select *OK* to save your changes and close the page.

To assign a client reputation profile to a device:

1. Right-click in the profile row and select *Assigned Devices* from the pop-up menu.
2. Add or remove devices as needed in the *Assigned Devices* dialog box, then select *OK*.

   The devices assigned to the profile are shown in the Assign To column on the Client reputation content pane.

Certificate Templates

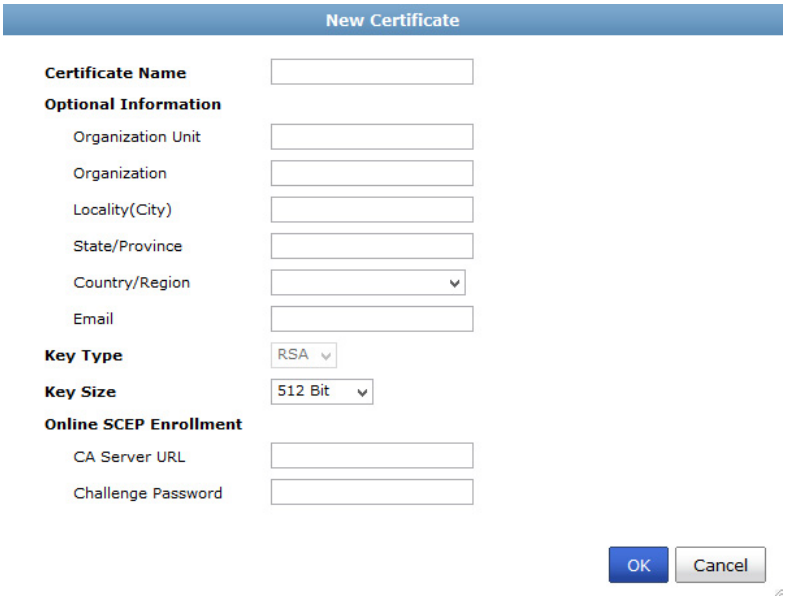
The certificate templates menu allows you to create certificate templates, add devices to them, and then generate certificates for selected devices. Once the certificates have been generated and signed, they can be installed using the install wizard.

To create a new certificate template:

1. In the *Provisioning Templates* tree menu, right-click on *Certificate Templates* and select *Create New* from the pop-up menu.

   The *New Certificate* dialog box opens.

Figure 110: New certificate template



2. Enter the following information:

Certificate Name	Enter a name for the certificate.
Optional Information	Optionally, enter the organization unit, organization, locality (city), province or state, country or region, and email address.
Key Type	Select the key type from the drop-down list.
Key Size	Select the key size from the drop-down list.
Online SCEP Enrollment	
CA Server URL	Enter the CA server URL.
Challenge Password	Enter the challenge password for the CA server.

3. Select *OK* to create the certificate.

To edit a certificate:

1. Right-click on the certificate name in the tree menu and select *Edit* from the pop-up menu.
2. Edit the settings as required in the *Edit Certificate* window, then select *OK* to apply the changes.

To delete a certificate:

1. Right-click on the certificate name in the tree menu and select *Delete* from the pop-up menu.
2. Select *OK* in the confirmation dialog box to delete the certificate.

To add device to a certificate template:

1. Select the certificate template from the tree menu to which you are adding devices.
2. In the content pane, select *Add Device* from the toolbar.

   The *Add Device* dialog box opens.
3. Add devices from the drop-down list, then select *OK* to add the devices.

To generate certificates:

1. Do one of the following:
   - Select one or more devices from the list of devices added to the certificate template, and then select *Generate* from the toolbar.
   - Right-click on a device from the list and select *Generate* from the pop-up menu.
2. Confirm the certificate generation in the confirmation dialog box to generate the certificate.

   If a certificate failed generation, you can attempt to generate the certificate again.

   If the certificate name already exists on the FortiGate unit, it will be overwritten each time the generate button is run. This allows the certificates to be updated more easily (for instances, if it has expired or is about to expire) without affecting any existing VPN configurations that are using the certificate.

FortiManager Wizards

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

FortiManager offers four wizards:

- Add device wizard
  - *Discover*: The device will be probed using the provided IP address and credentials to determine the model type and other important information.
  - *Add Model Device*: The device will be added using the chosen model type and other explicitly entered information.
- Install wizard
  - *Install Policy Package & Device Settings*: Install a specific policy package. Any device specific settings for devices associated with the package will also be installed.
  - *Install Device Settings (only)*: Install only device settings for a selected set of devices; policy and object changes will not be updated from the last install.
- Import policy wizard
  - *Import device*
- Quick install
  - *Re-install Policy Package*: You can right-click on the Config Status column icon to perform a quick install of a policy package without launching the Install wizard.

This section will describe each wizard and their usage.



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

Add device wizard

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

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

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

A shortened version of the *Add Device* wizard can also be used to import policies to an already installed or imported device. See “Import policy wizard” on page 231.

Launching the add device wizard

To launch the Add Device wizard, right-click on an item in the *Device Manager* tree-menu then select *Add Device* from the pop-up menu.

The *Add Device* wizard opens.



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

Add device wizard options

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

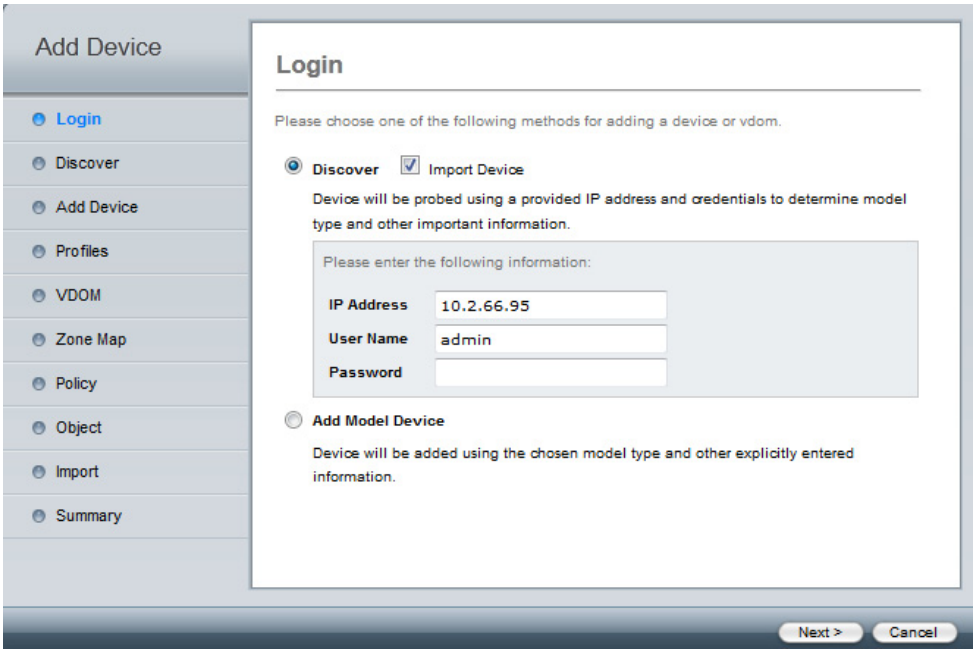
Discover

You will require the IP address of the unit you wish to add, as well as the unit's login and password. The device is probed using the provided IP address and credentials to determine model type and other important information. See "Adding a device" on page 147.

Import device

This option allows you to import a device and bring all of its policies and objects into the FortiManager system. You will require the IP address of the unit you wish to import, as well as the unit's login and password. Select *Import Device* to use this method. See "To add a device using Add Device wizard (Discovery mode):" on page 209.

Figure 111: Discover mode



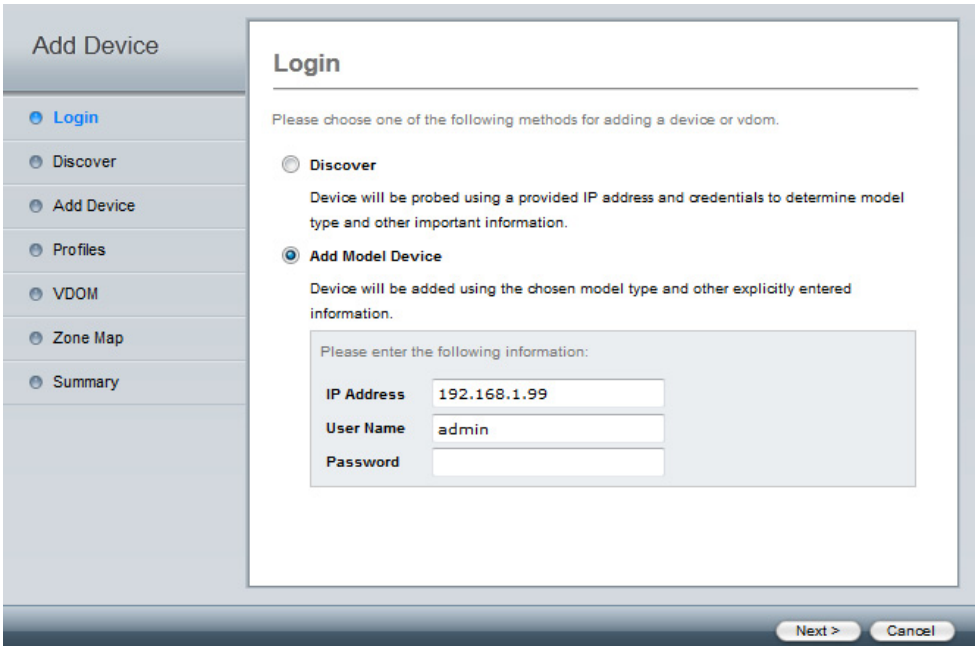
The following options are available:

Discover	Device will be probed using a provided IP address and credentials to determine model type and other important information.
Import Device	Select to Import device policies and objects.
IP Address	Enter the device IP address. This IP will be probed to complete the import.
User Name	Enter the user name for the device.
Password	Enter the password for the device.

Add model device

If you have a new unit you wish to install, but it is not yet online, you can use this feature to add it to your FortiManager. You must have all related information about the unit to use this feature. See “Adding a device” on page 147.

Figure 112: Add model device mode



Enter the following information:

Add Model Device	Device will be added using the chosen model type and other explicitly entered information.
IP Address	Enter the device IP address. This IP address can be changed if the IP address changes at the time of installation.
User Name	Enter the user name for the device.
Password	Enter the password for the device (optional).

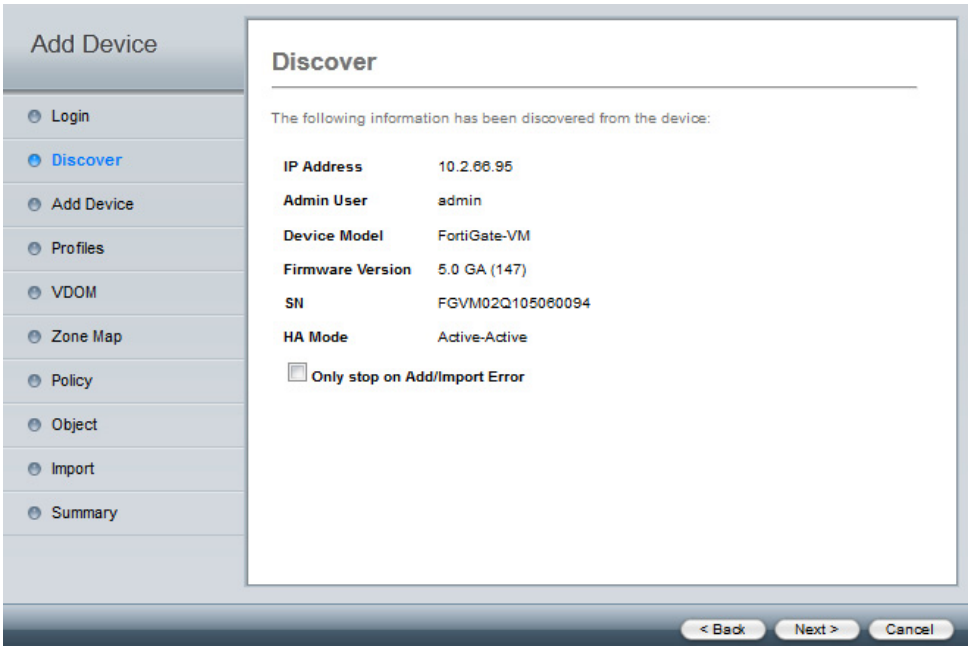
Add a device using the add device wizard (Discovery mode)

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

To add a device using Add Device wizard (Discovery mode):

1. Launch the *Add Device* wizard.
2. Select *Discover*, and enable *Import Device* on the *Login* phase page.
3. Enter the IP address, user name and password for the device, and select *Next*.
4. The FortiManager will probe the IP address on your network to discover device details, including:
   - IP address
   - Administrative user name
   - Device model
   - Firmware version (build)
   - Serial number
   - High Availability mode

Figure 113: Discover phase

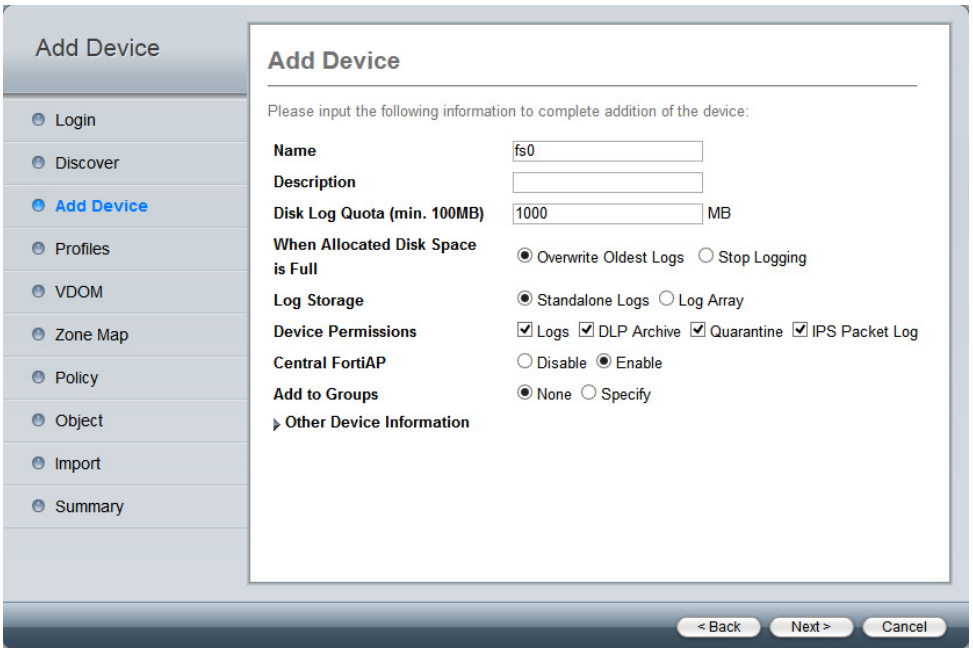


Only stop on Add/Import Error	Enable the option *Only stop on Add/Import Error*, if you would like the wizard to stop when encountering this error.

5. Select *Next* to continue.

6. Enter the following information:
   - Name
   - Description
   - Disk log quota
   - Behavior when disk is full
   - Device permissions
   - Group information
   - Device contact information

Figure 114: Add device phase



Name	Enter a name for the device.
Description	Enter a description of the device (optional).
Disk Log Quota	Enter a value for the disk log quota in MB.
When Allocated Disk Space is Full	Specify what action to take when the disk space is full: • *Overwrite Oldest Logs* • *Stop Logging*
Log Storage	Specify the log storage method, either *Standalone Logs* or *Log Array*.
Device Permissions	Specify device permissions: • *Logs* • *DLP Archive* • *Quarantine* • *IPS Packet Log*

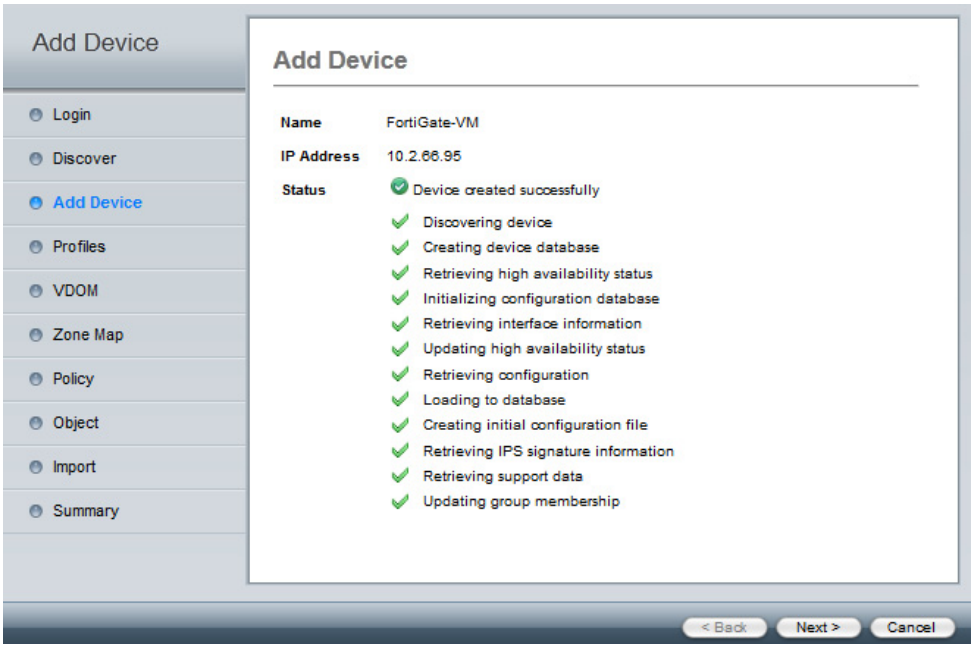
Add to Groups	Select to add the device to any predefined groups.
Other Device Information	Enter other device information (optional), including: • *Company/Organization* • *Contact* • *City* • *Province/State* • *Country*

7. Select *Next*.

   The wizard will proceed to discover the device, and perform some or all of the following checks:

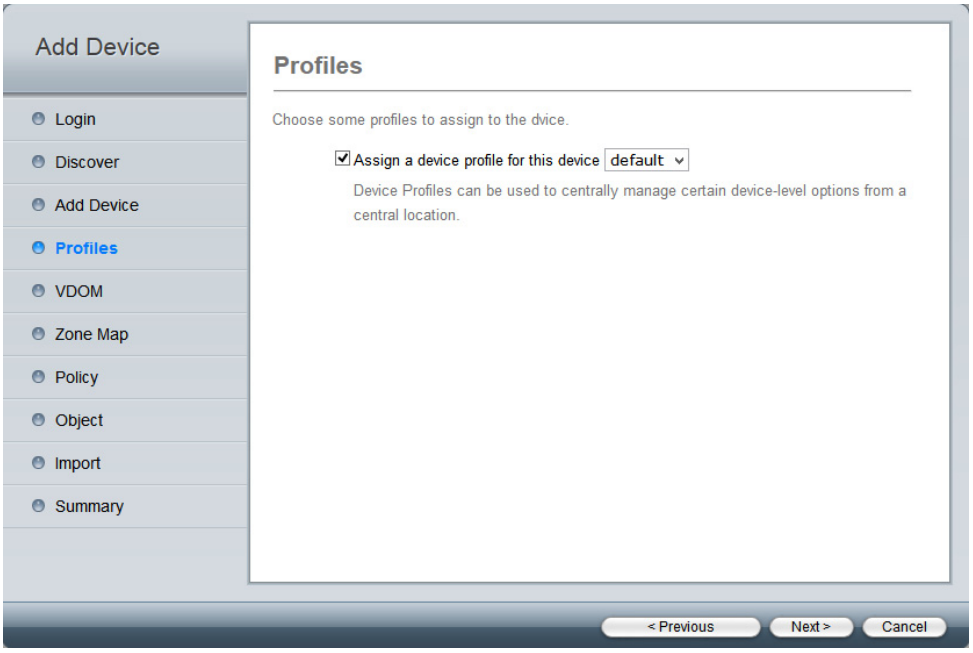
   - Discovering device
   - Creating device database
   - Retrieving high availability status
   - Initializing configuration database
   - Retrieving interface information
   - Updating high availability status
   - Retrieving configuration
   - Loading to database
   - Creating initial configuration file
   - Retrieving IPS signature information
   - Retrieving support data
   - Updating group membership

Figure 115: Device created successfully



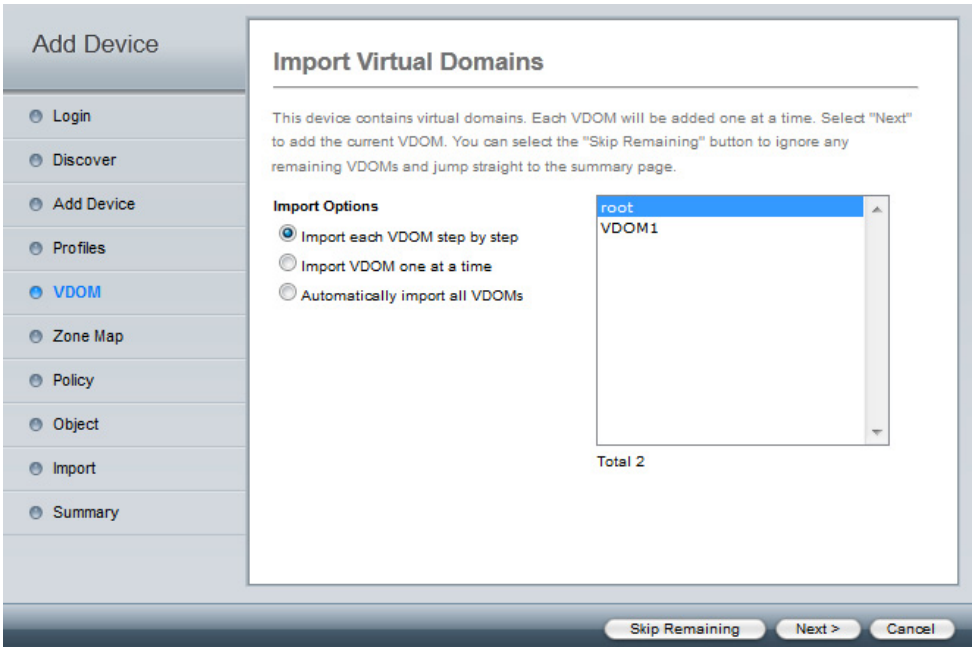
8. Device profiles can be used to centrally manage certain device-level options from a central location. You can assign a device profile using the drop-down menu. Alternatively, you can select to configure all settings per-device inside *Device Manager*.

Figure 116: Device profile phase



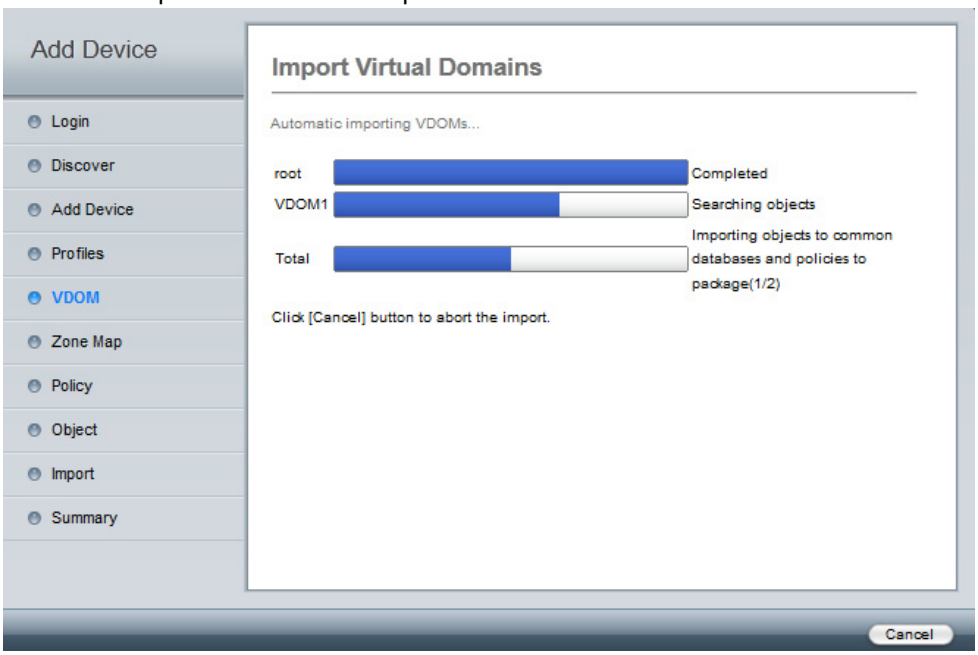
9. Select *Next* to continue.
10. If VDOMs are not enabled on the device, the wizard will skip the VDOM phase. You can Select to import each VDOM step by step, one at a time, or automatically import all VDOMs.

Figure 117: Import virtual domains phase



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

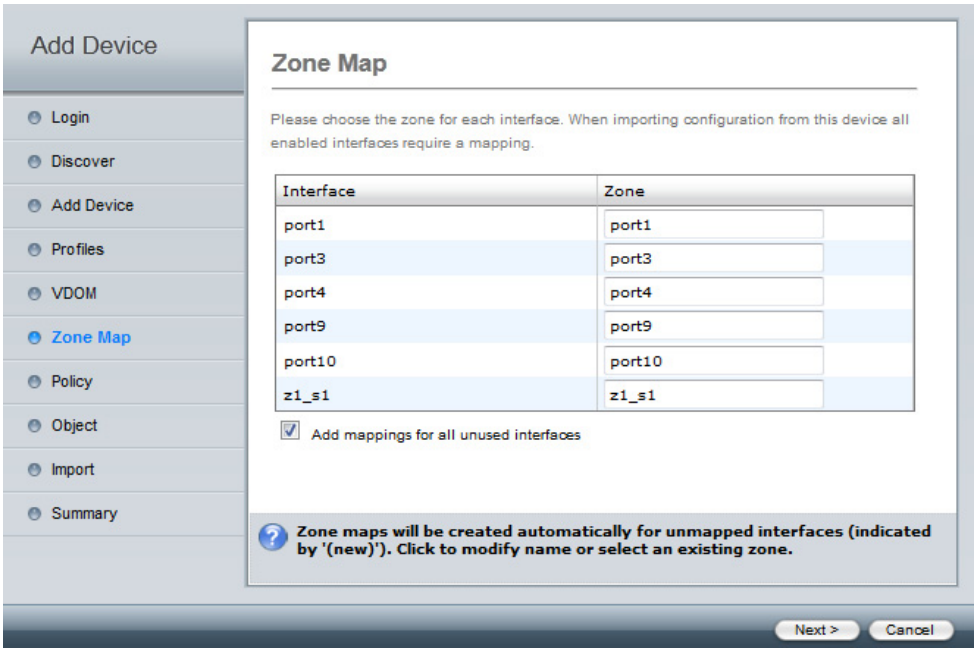
Table 12: Import virtual domains phase



11. You can use the global zone map section of the wizard to map your dynamic interface zones.

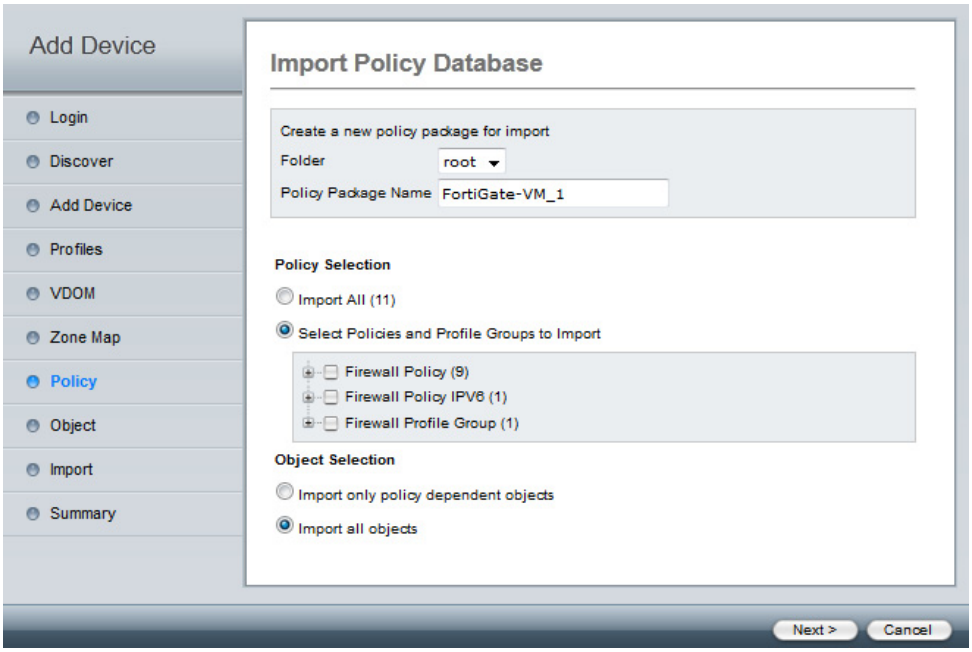
When importing configurations from a device, all enabled interfaces require a mapping.

Figure 118: Zone map phase



12. Select *Next* to continue. The wizard will then perform a policy search to find all policies in preparation for importation into FortiManager's database. Once this step is complete, you will be shown a summary of the policies. Choose a folder on the drop-down list, enter a new policy package name, and select the policies you would like to import from the list. You can also select to import only policy dependent objects or import all objects.

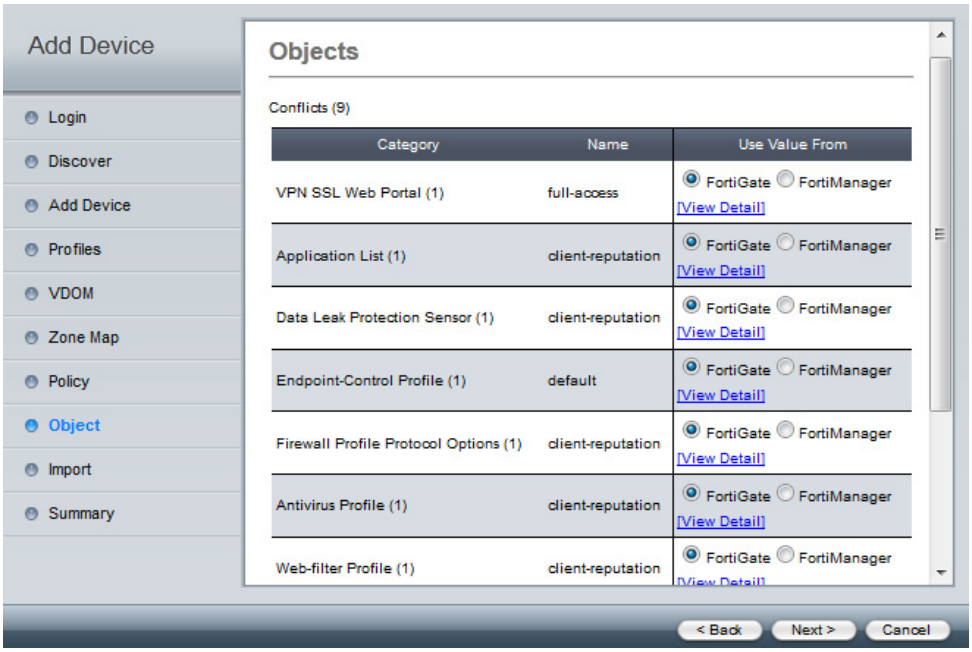
Figure 119: Import policy database phase



Folder	Select the folder using the drop-down list.
Policy Package Name	Enter a *Policy Package Name* (if required).
Policy Selection	
Import All	Select to import all policies.
Select Policies and Profile Groups to Import	Select to import specific policies and profile groups on the tree-menu.
Object Selection	
Import only policy dependent objects	Select to import policy dependent objects only for the device.
Import all objects	Select to import all objects for the selected device.

13. Select *Next* to continue. The wizard then searches the unit for objects to import, and reports any conflicts it detects. If conflicts are detected, you can decide whether to use the FortiGate value or the FortiManager value.

Figure 120: Object phase



14. If conflicts occur, you can scroll down on this page to download the conflict file. This file is HTML-based and provides details of conflicts.

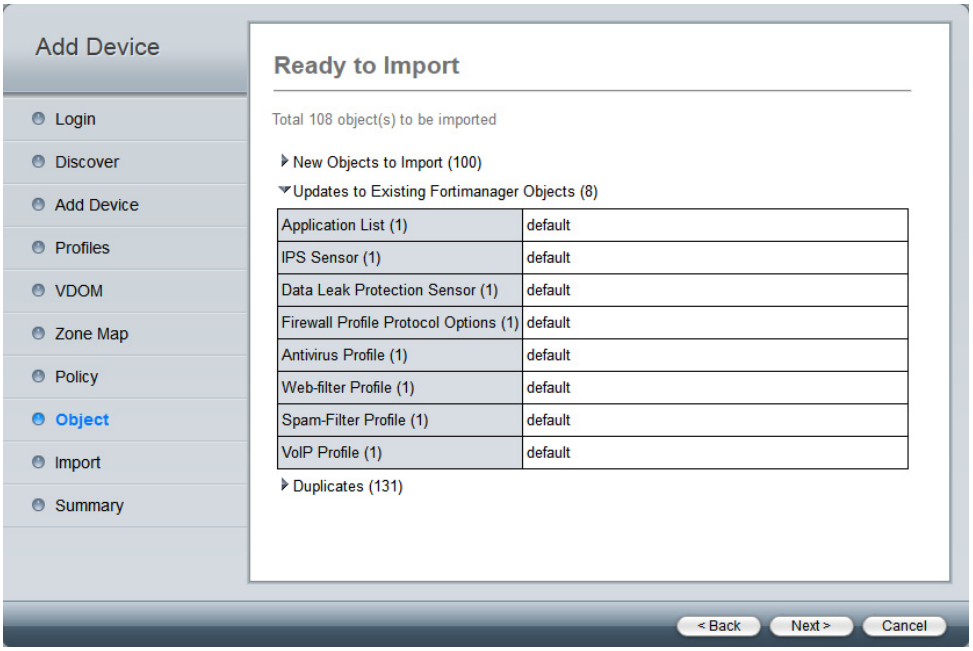
Figure 121: Download conflict file

Category	Name	Attribute	FortiGate	FortiManager
Antivirus Profile	client-reputation	comment	client reputation AV profile	scan and delete virus
Application List	client-reputation	comment	client reputation application list	monitor all applications
Data Leak Protection Sensor	client-reputation	comment	client reputation DLP sensor	summary archive email and web traffic
Endpoint-Control Profile	default	**endpoint_control_prof_fct_winmac_set**		
		forticlient-log-upload-schedule	daily	
Firewall Profile Protocol Options	client-reputation	**fw_prof_protocol_options_https**		
		ports	0	443
		options		no-content-summary
		fw_prof_protocol_options_imaps		
		ports	0	993
		options		fragmail no-content-summary
		fw_prof_protocol_options_pop3s		
		ports	0	995
		options		fragmail no-content-summary
		fw_prof_protocol_options_smtps		
		ports	0	465
		options		fragmail no-content-summary splice
		fw_prof_protocol_options_ftps		
		ports	0	990
		options		no-content-summary splice
		comment	client reputation services	client-reputation
Spam-Filter Profile	client-reputation	comment	client reputation filtering	client-reputation malware and phishing URL filtering

15. Select *Next*.

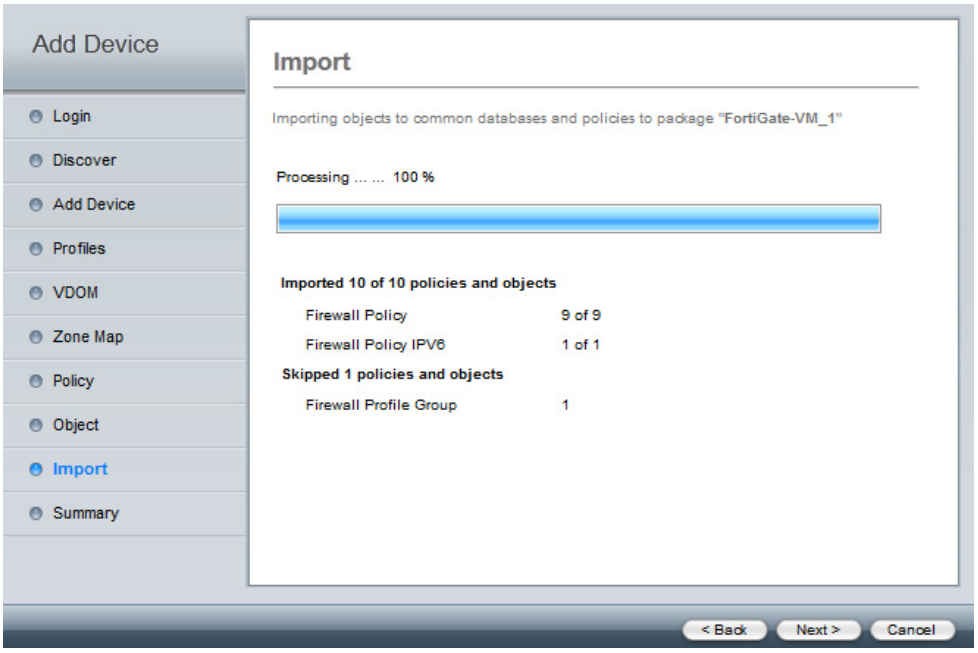
The objects that are to be imported will be shown.

Figure 122: Objects to import



16. Select *Next* to import policies and objects into the database.

Figure 123: Import phase



17. Select *Next*.

The wizard will present a message *Discovered Device Added Successfully* and provides a detailed summary of the import. You can select to download the import report. This report is only available on this page.

Figure 124: Summary phase



Figure 125: Import report sample

```
Start to import config from device(140) vdom(root) to adom(3)
"firewall schedule recurring",SUCCESS,"(name=always, oid=465,
DUPLICATE)"
"firewall address",SUCCESS,"(name=all, oid=300, DUPLICATE)"
"firewall address",SUCCESS,"(name=ad1, oid=460)"

"firewall addrgrp",SUCCESS,"(name=adgr1, oid=461)"

"firewall ippool",SUCCESS,"(name=pool1, oid=462)"

"firewall central-nat",SUCCESS,"(name=ID:1 (#1), oid=495)"

"firewall profile-protocol-options",SUCCESS,"(name=default, oid=
326)"

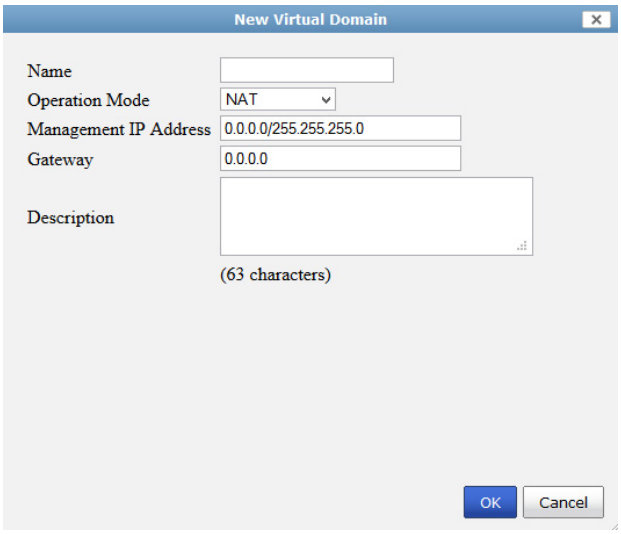
"antivirus profile",SUCCESS,"(name=default, oid=433, DUPLICATE)"
"firewall policy",SUCCESS,"(name=ID:1 (#1), oid=493)"
"firewall policy",SUCCESS,"(name=ID:2 (#2), oid=494)"
```

18. Select *Finish* to close the wizard.

Add a VDOM

To add a VDOM to a managed FortiGate device, right-click on the content pane for a particular device and select *Add VDOM* from the pop-up menu.

Figure 126: Add a VDOM



Name	Enter a name for the new virtual domain.
Operation Mode	Select either NAT or Transparent for operation mode.
Management IP Address	Enter the management IP address for the VDOM.
Gateway	Enter the gateway.
Description	Enter a description. (Optional)

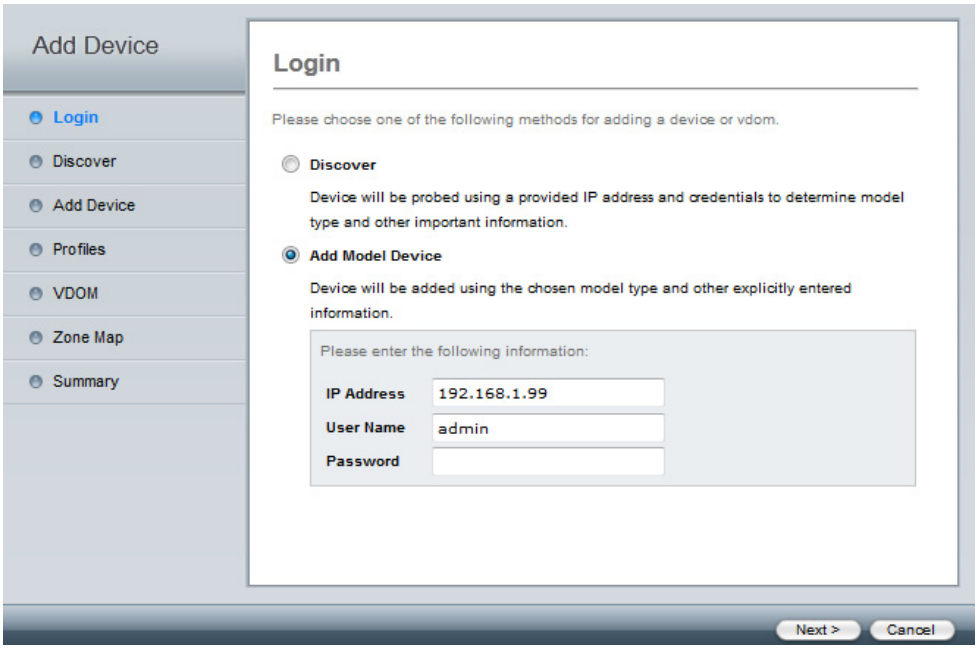
Add a device using the add device wizard (Add model device)

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

To add a model device:

1. Right-click the tree-menu or right content pane to launch the *Add Device* wizard.
2. Select *Add Model Device* on the *Login* phase page.
3. Enter the IP address, user name and password for the device, and select *Next*.

Figure 127: Login phase



Enter the following information:

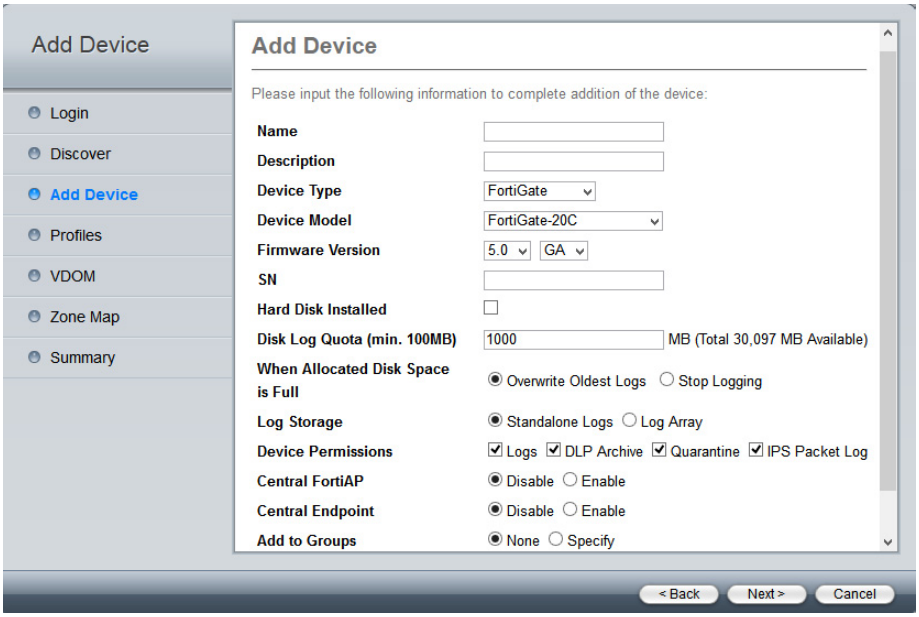
Add Model Device	Device will be added using the chosen model type and other explicitly entered information.
IP Address	Enter the device IP address. This IP address can be changed if the IP address changes at the time of installation.
User Name	Enter the user name for the device.
Password	Enter the password for the device. (optional)

4. Select *Next* to continue.



If the device does not support interface mode, the option to enable this feature will not be available.

Figure 128: Add device phase



5. Complete the following fields:

Name	Enter a name for the device.
Description	Enter a description for the device (optional).
Device Type	Select the device type on the drop-down list.
Device Model	Select the device model on the drop-down list.
Firmware Version	Select the firmware version and major release on the drop-down list.
Serial Number	Enter the device serial number. This value must match the device model selected.
Enable Interface Mode	Select to enable interface mode. If the device does not support interface mode, this option is not available.
Hard Disk Installed	This option is available when the device model has a hard disk.
Disk Log Quota.	Enter the disk log quota in MB.
When Allocated Disk Space is Full	Select to overwrite oldest logs or stop logging when the allocated disk space is full.
Device Permissions	Specify device permissions: • Logs • DLP Archive • Quarantine • IPS Packet Log
Central FortiAP	Enable or disable central FortiAP.
Central Endpoint	Enable or disable central endpoint control.

Add to Groups	Select to add the device to any predefined groups.
Other Device Information	Enter other device information including: • Company/Organization • Contact • City • Province/State • Country

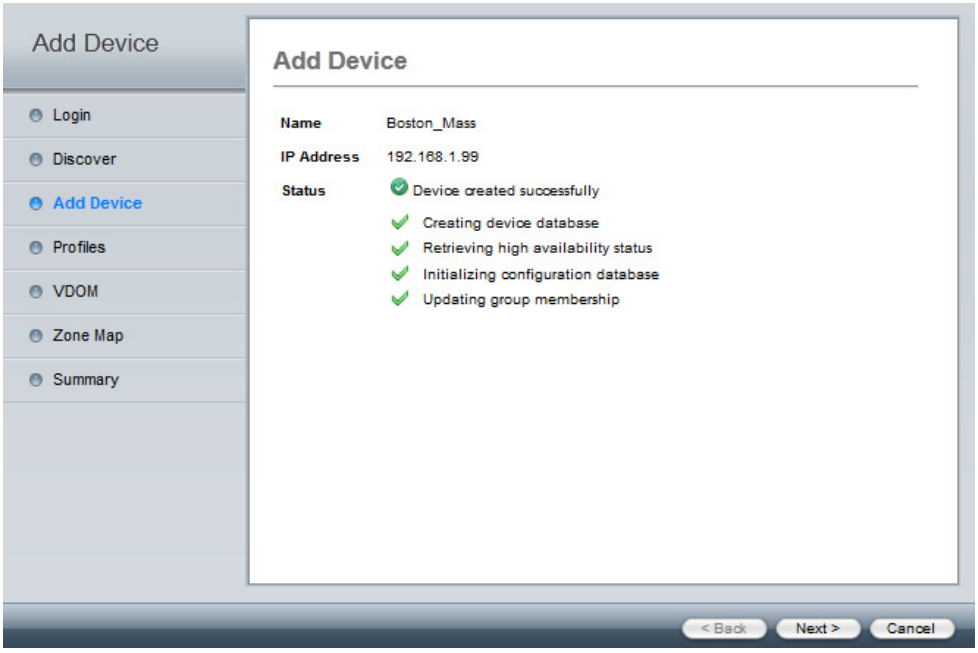
Not all device models are supported in all firmware versions. If you are unable to find the device model under one firmware version, it might be available under a newer version.

Each device must have a unique name, otherwise the wizard will fail.

6. Select *Next*.

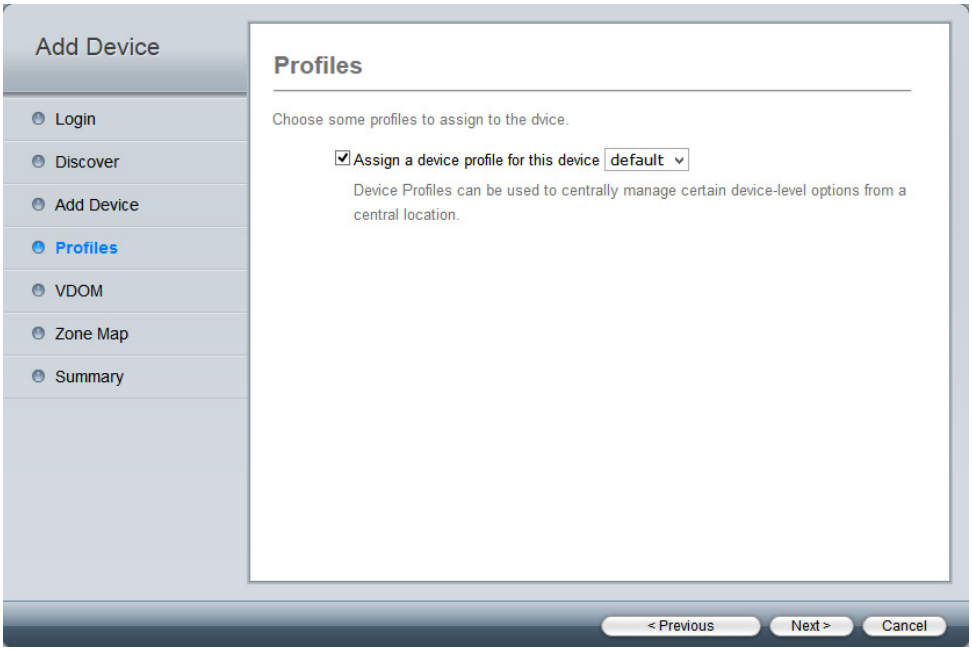
   The device will be created in the FortiManager database.

Figure 129: Device created successfully



7. Device profiles can be used to centrally manage certain device-level options from a central location. You can assign a device profile using the drop-down menu. Alternatively, you can select to configure all settings per-device inside *Device Manager*.

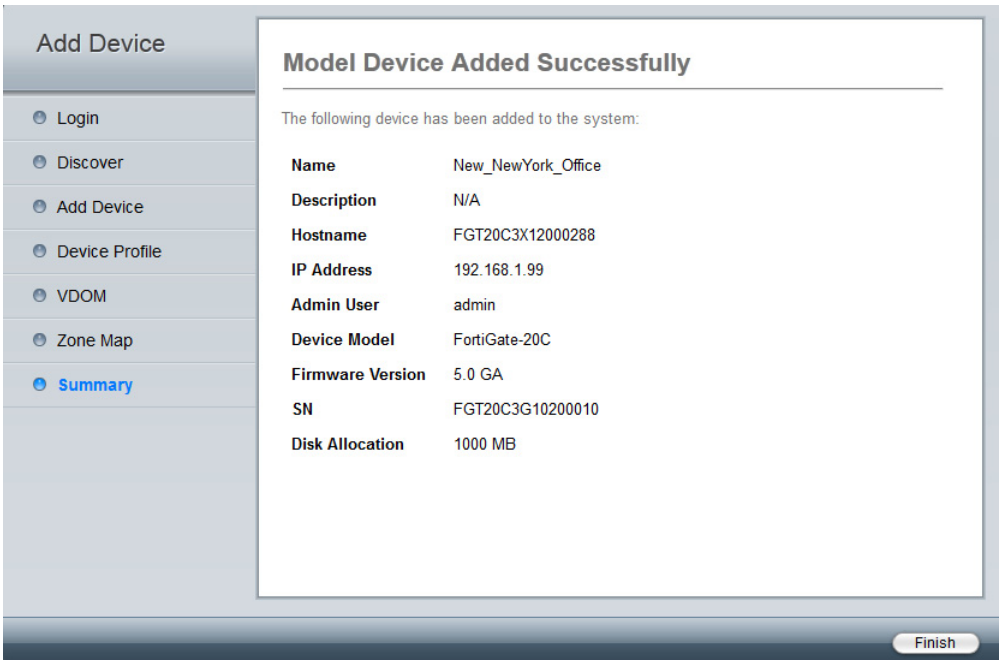
Figure 130: Device profile phase



8. Select *Next*.

   The *Add Model Device* wizard proceeds to the summary page.

Figure 131: Summary phase



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

Install wizard

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

Launching the install wizard

To launch the *Install* wizard right-click on the *Device Manager* tree-menu and select *Install* from the pop-up menu.

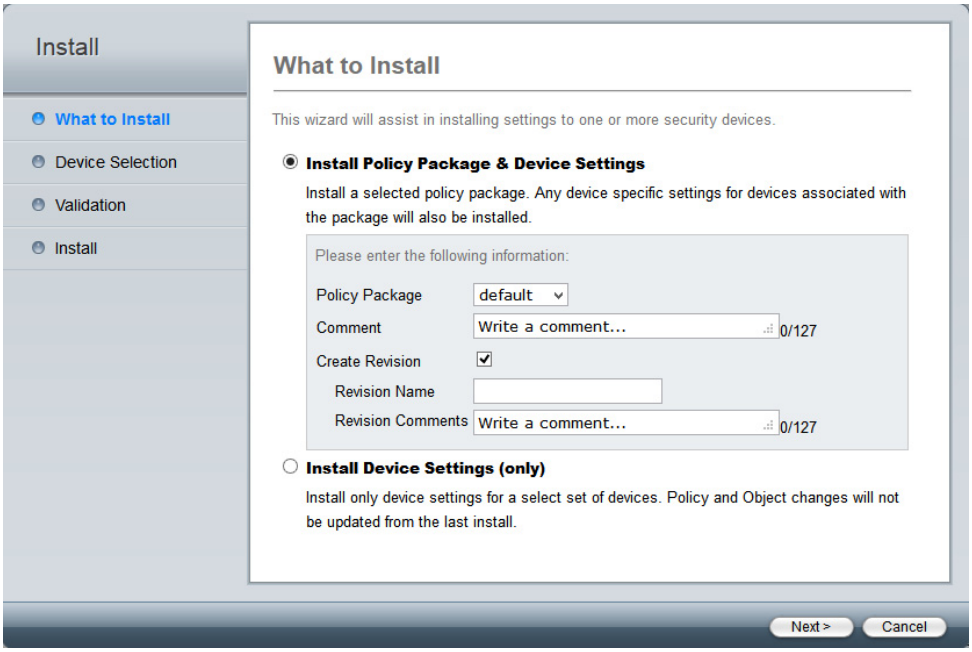
The *Introduction* phase gives you two options for installing settings:

- Install policy package and device settings: Install a selected policy package. Any device specific settings for devices associated with package will also be included.
- Installing device settings: Install only device settings for a select set of devices. Policy and object changes will not be updated from the last install.

Install policy package and device settings

Select *Install Policy Package & Device Settings*, select the policy package on the drop-down list, and optionally, enter a comment for the policy package being installed and create a revision.

Figure 132: Install policy package and device settings



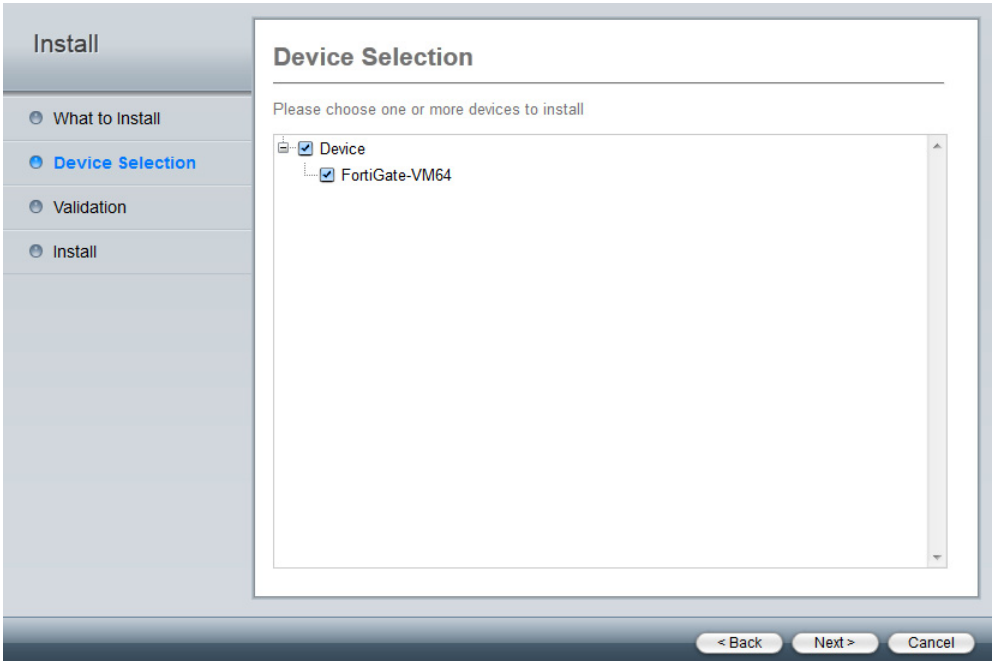
Configure the following:

Policy Package	Select the policy package from the drop-down list.
Comment	Enter an optional comment.
Create Revision	Select the checkbox to create a revision.
Revision Name	Enter the revision name.
Revision Comments	Enter an optional comment.

Device selection

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

Figure 133: Device selection phase



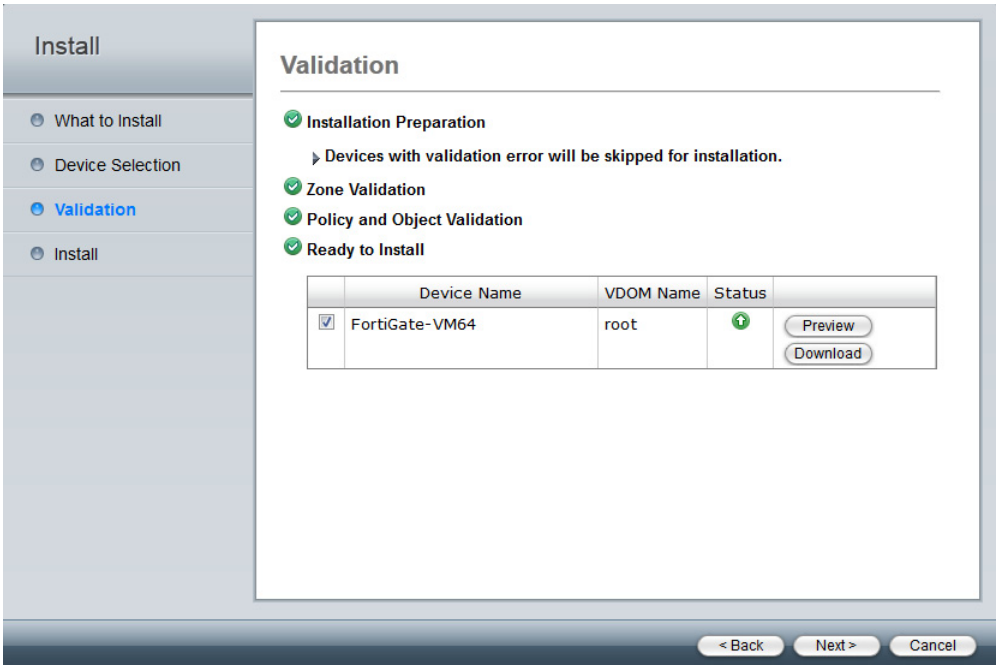
Validation

The *Validation* phase checks the following:

- Installation Preparation
- Zone Validation
- Policy and Object Validation

Devices with a validation error will be skipped for installation.

Figure 134: Validation phase



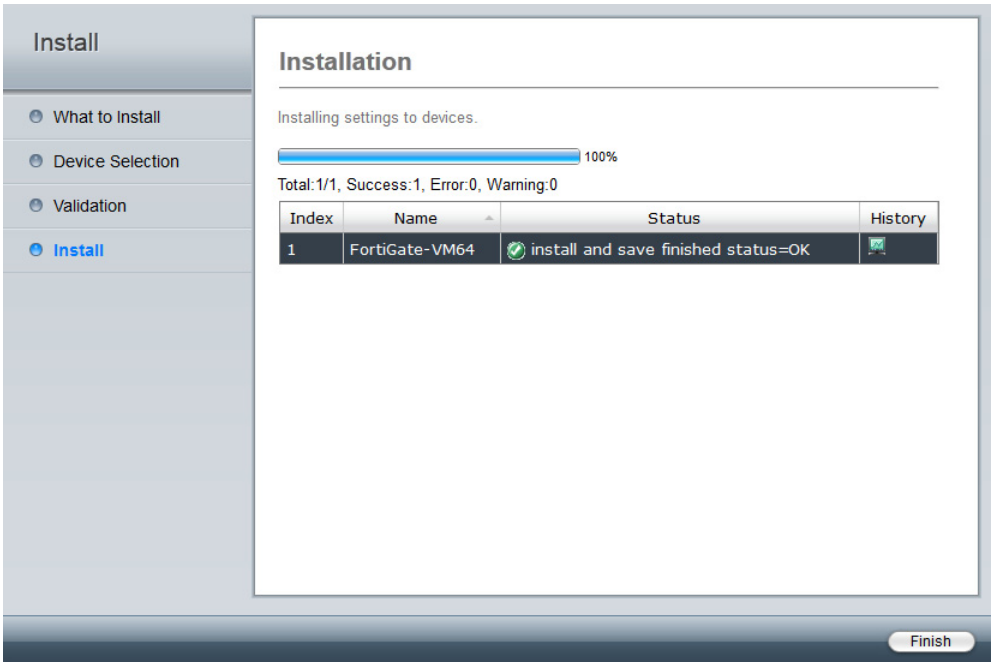
Available actions:

Preview	Select to view device preview.
Download	Select download to open or save the preview file in `.txt` format.

Installation

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

Figure 135: Policy package installation window



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

Figure 136: Device installation history

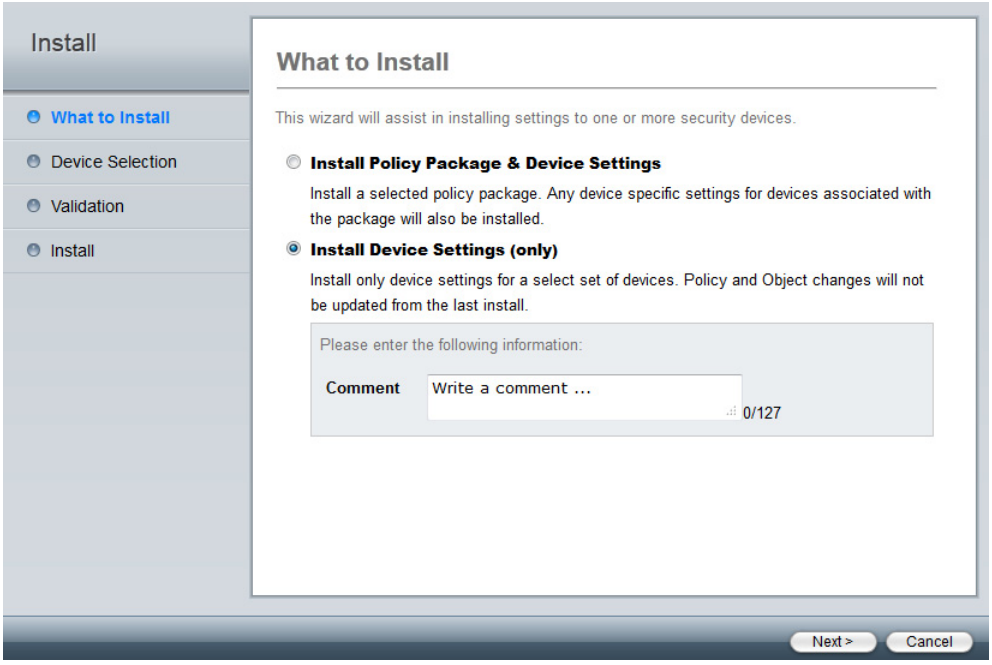
Task: 60, Record:1

Name	Percentage	Description
FortiGate-VM64	0%	start to install dev(FortiGate-VM64)
FortiGate-VM64	15%	init state: start to get pre-checksum
FortiGate-VM64	25%	get pre-checksum state: start get diff(chkout=1)
FortiGate-VM64	35%	No cmds to be installed
FortiGate-VM64	100%	install and save finished status=OK

Installing device settings

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

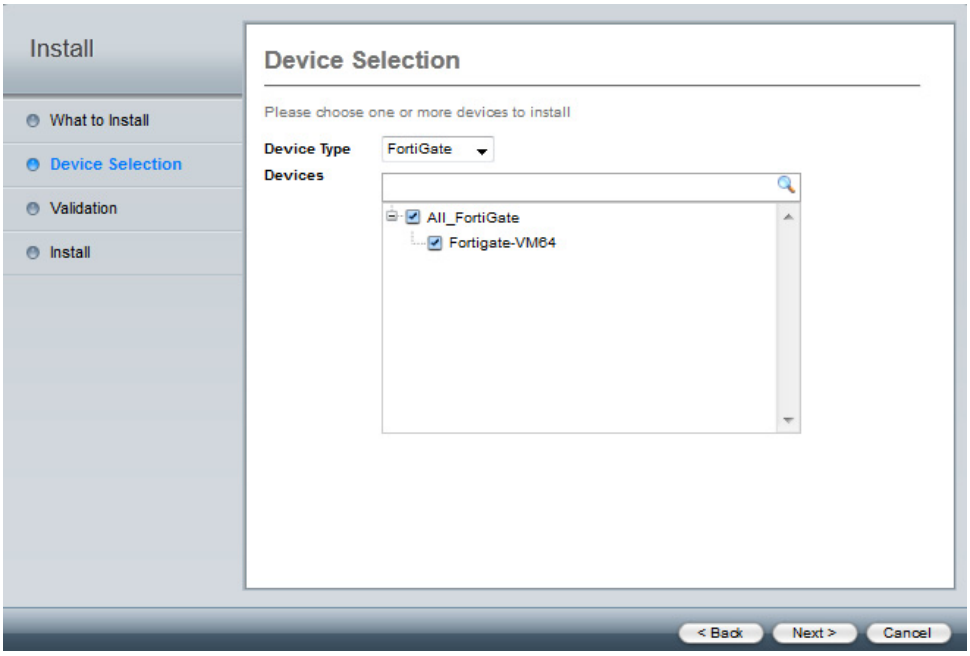
Figure 137: Install device settings only



Device selection

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

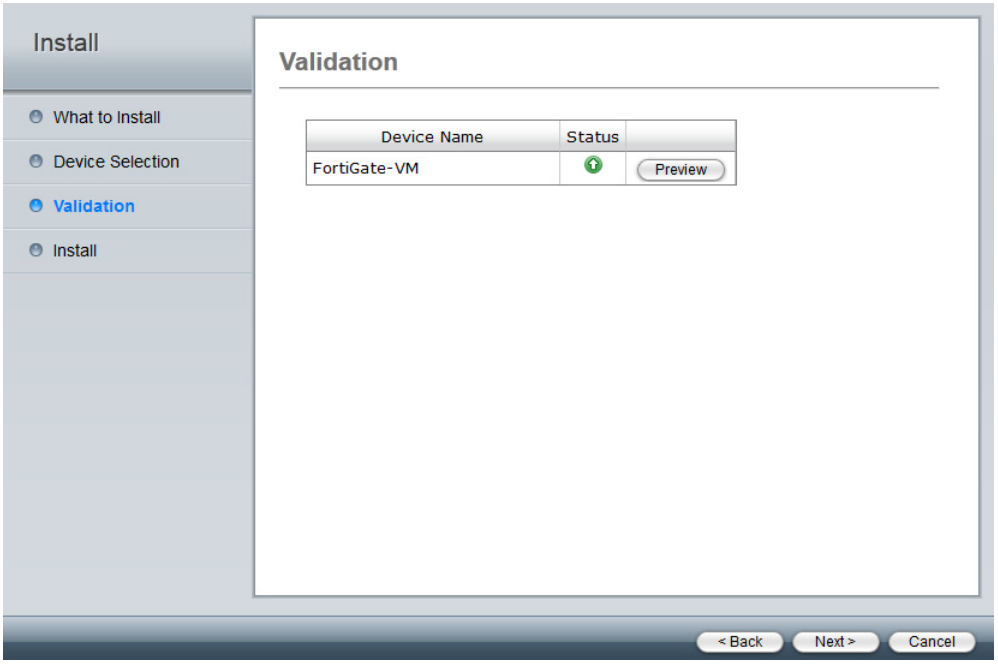
Figure 138: Device selection window



Validation

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

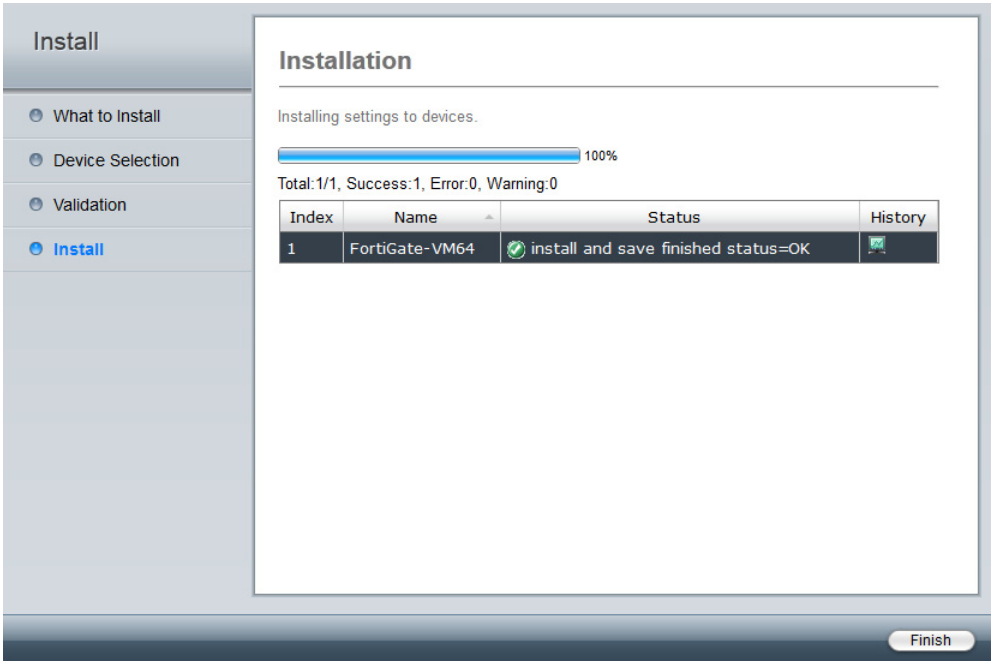
Figure 139: Validation phase



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 140: Device settings successful installation window



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

Figure 141: Device installation history

Task: 60, Record:1

Name	Percentage	Description
FortiGate-VM64	0%	start to install dev(FortiGate-VM64)
FortiGate-VM64	15%	init state: start to get pre-checksum
FortiGate-VM64	25%	get pre-checksum state: start get diff(chkout=1)
FortiGate-VM64	35%	No cmds to be installed
FortiGate-VM64	100%	install and save finished status=OK

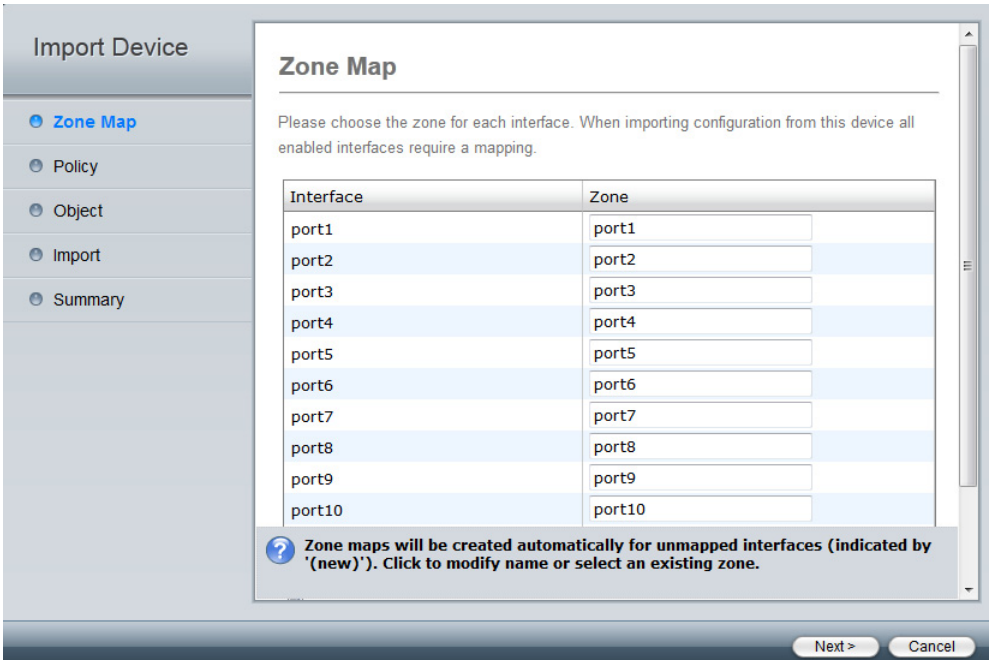
Import policy wizard

You can right-click on the right-content pane and select *Import Policy* to launch the Import Device wizard. This wizard will allow you to import zone maps, policy database,

Zone map

The Zone Map phase allows you to choose a zone for each interface. When importing configuration from this device all enabled interfaces require a mapping. Zone maps will be created automatically for unmapped interfaces.

Figure 142: Zone map phase

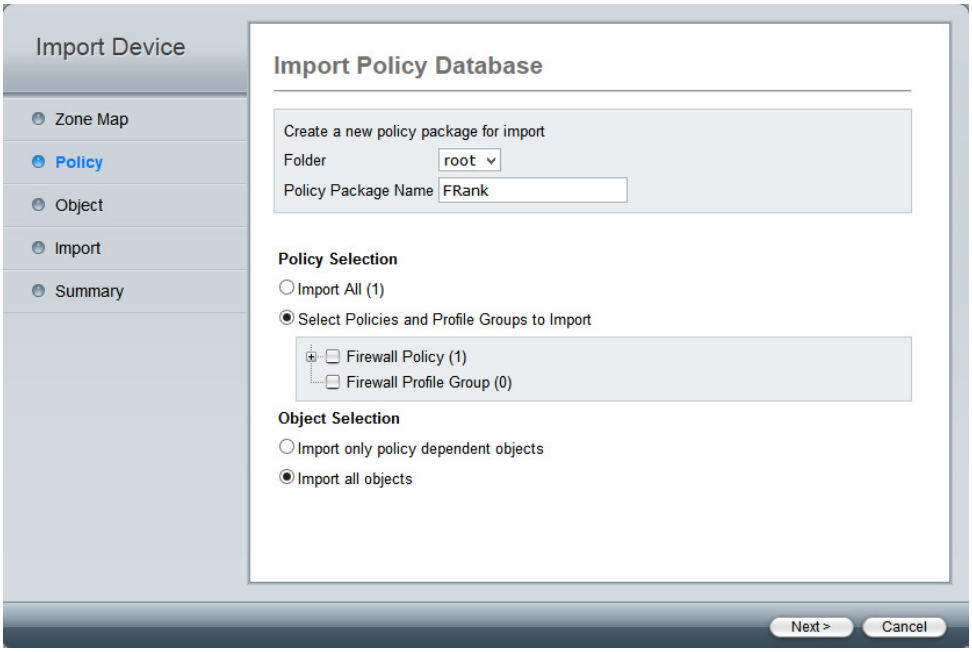


Add mappings for all unused interfaces	Select to automatically create zone maps for unused interfaces.

Policy

The policy phase allows you to create a new policy package for import. Select the folder on the drop-down menu, and specify the policy package name. You can select to import all policies for select specific policies and profile groups to import.

Figure 143: Policy phase

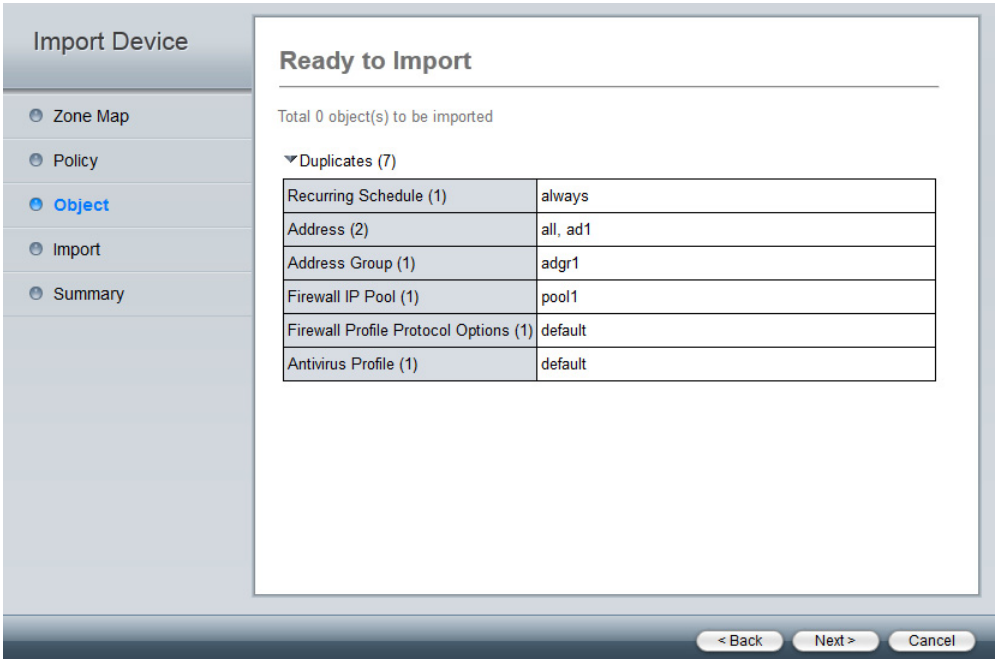


Folder	Select a folder on the drop-down menu.
Policy Package Name	Enter a name for the policy package.
Policy Selection	Select to import all, or select specific policies and policies groups to import.
Object Selection	Select *Import only policy dependent objects* to import policy dependent objects only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

Object

The object phase will search for dependencies. Duplicates will not be imported.

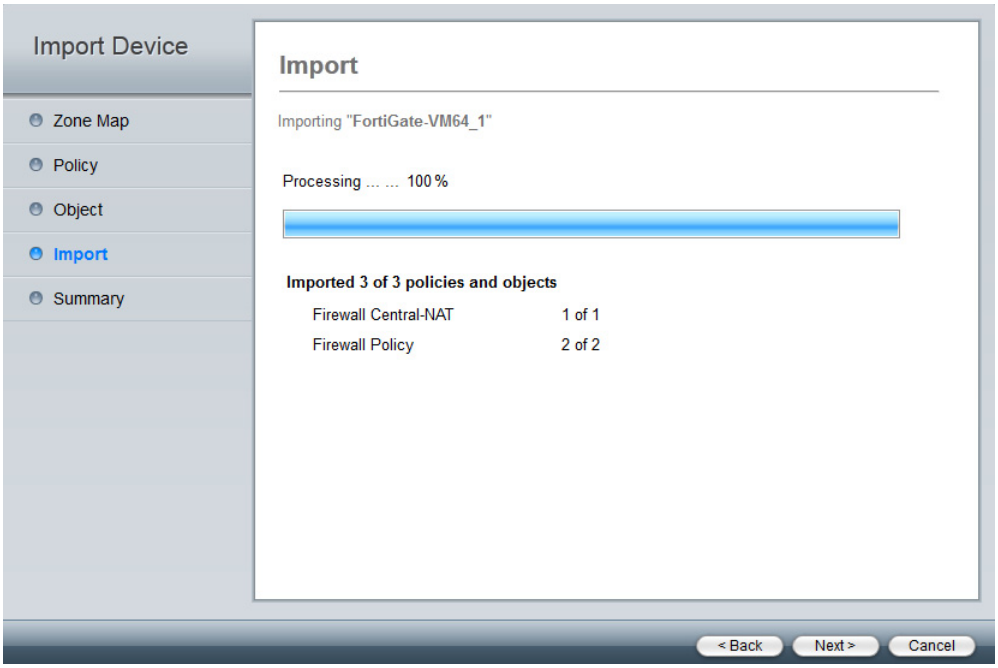
Figure 144: Object phase



Import

The import phase will import zone map, policies, and objects into the FortiManager database.

Figure 145: Import phase



Summary

The summary phase allows you to download and view the import device summary results.

Figure 146: Summary phase

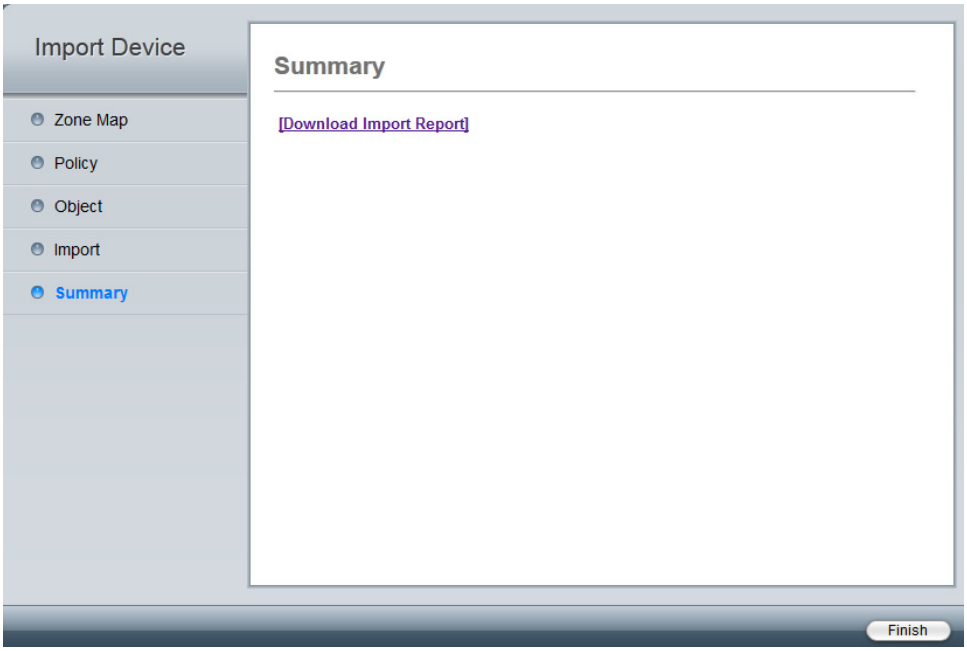


Figure 147: Summary example

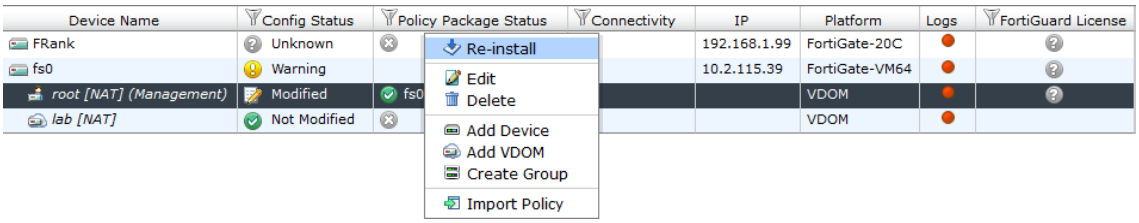
```
Start to import config from device(140) vdom(root) to adom(3)
"firewall schedule recurring",SUCCESS,"(name=always, oid=465,
DUPLICATE)"
"firewall address",SUCCESS,"(name=all, oid=300, DUPLICATE)"
"firewall address",SUCCESS,"(name=ad1, oid=302, DUPLICATE)"
"firewall addrgrp",SUCCESS,"(name=adgr1, oid=304, DUPLICATE)"
"firewall ippool",SUCCESS,"(name=pool1, oid=466, DUPLICATE)"
"firewall central-nat",SUCCESS,"(name=ID:1 (#1), oid=495)"

"firewall profile-protocol-options",SUCCESS,"(name=default, oid=
467, DUPLICATE)"
"antivirus profile",SUCCESS,"(name=default, oid=433, DUPLICATE)"
"firewall policy",SUCCESS,"(name=ID:1 (#1), oid=493)"
"firewall policy",SUCCESS,"(name=ID:2 (#2), oid=494)"
```

Quick install

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

Figure 148: Select re-install



Device Configurations

The FortiManager system maintains a configuration repository to manage device configuration revisions. After modifying device configurations, you can save them to the FortiManager repository and install the modified configurations to individual devices or device groups. You can also retrieve the current configuration of a device, or revert a device's configuration to a previous revision.

This section contains the following topics:

- Checking device configuration status
- Managing configuration revision history

Checking device configuration status

In the *Device Manager* tab, when you select a device, you can view that device's basic information under the *device dashboard*. You can also check if the current configuration file of the device stored in the FortiManager repository is in sync with the one running on the device.

If you make any configuration changes to a device directly, rather than using the FortiManager system, the configuration on the device and the configuration saved in the FortiManager repository will be out of sync. In this case, you can re synchronize with the device by retrieving the configuration from the device and saving it to the FortiManager repository.

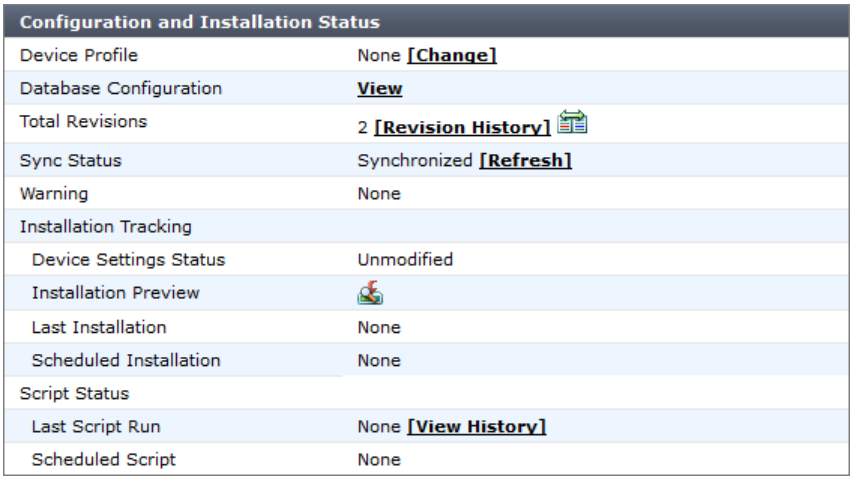
You can use the following procedures when checking device configuration status on a FortiGate, FortiCarrier, or FortiSwitch.

To check the status of a configuration installation on a FortiGate unit:

1. Go to the Device Manager tab, then select the ADOM and device group.
2. On the *All FortiGate* page, select the FortiGate unit that you want to check the configuration status of.

   The device dashboard of for that unit is shown in the lower content pane.
3. On the dashboard, locate the *Configuration and Installation Status* widget.
4. Verify the status in the *Installation Tracking* section.

Figure 149: Configuration and Installation Status widget



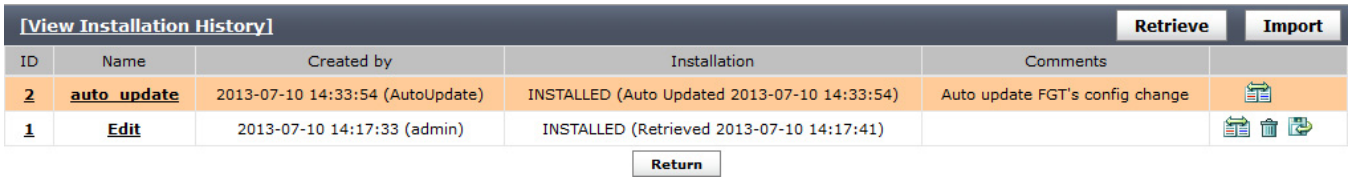
The following information is shown:

Device Profile	The device profile associated with the device. Select *Change* to set this value.
Database Configuration	Select *View* to display the configuration file of the FortiGate unit.
Total Revisions	Displays the total number of configuration revisions and the revision history. Select *Revision History* to view device history.
Sync Status	The synchronization status with the FortiManager. • *Synchronized*: The latest revision is confirmed as running on the device. • *Out_of_sync*: The configuration file on the device is not synchronized with the FortiManager system. • *Unknown*: The FortiManager system is unable to detect which revision (in revision history) is currently running on the device. • Select *Refresh* to update the Installation Status.
Warning	Displays any warnings related to configuration and installation status. • *None*: No warning. • *Unknown configuration version running on FortiGate: FortiGate configuration has been changed!*: The FortiManager system cannot detect which revision (in *Revision History*) is currently running on the device. • *Unable to detect the FortiGate version*: Connectivity error! • *Aborted*: The FortiManager system cannot access the device.
Installation Tracking	
Device Settings Status	• *Modified*: Some configuration on the device has changed since the latest revision in the FortiManager database. Select *Save Now* to install and save the configuration. • *UnModified*: All configuration displayed on the device is saved as the latest revision in the FortiManager database.
Installation Preview	Select icon to display a set of commands that will be used in an actual device configuration installation in a new window.
Last Installation	*Last Installation*: The FortiManager system sent a configuration to the device at the time and date listed.
Scheduled Installation	*Scheduled Installation*: A new configuration will be installed on the device at the date and time indicated.
Script Status	Select Configure to view script execution history.
Last Script Run	Displays the date when the last script was run against the managed device.
Scheduled Script	Displays the date when the next script is scheduled to run against the managed device.

Managing configuration revision history

On the *Device Manager* tab, select a device on the tree-menu. On the device dashboard *Configuration and Installation Status* widget, select *Revision History* in the *Total Revisions* row, to view the FortiManager repository.

Figure 150: 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 240.
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 239 and "To download a configuration file to a local computer:" on page 240.
Name	A name added by the user to make it easier to identify specific configuration versions. You can select a name to edit it and add comments.
Created by	The time and date when the configuration file was created, and the person who created the file.
Installation	Display whether a configuration file has been installed or is currently active. The installation time and date is displayed. N/A status indicates that a particular revision was not sent to the device. The typical situation is that the changes were part of a later revision that was sent out to the device. For example, you make some changes and commit the changes. Now you have a revision called ID1. Then you make more changes and commit the changes again. Then you have a revision called ID2, which also includes the changes you made in revision ID1. If you install revision ID2, then the status of revision ID1 becomes N/A.

Comments	Display the comment added to this configuration file when you edit the file name.
Diff icon	Show only the changes or differences between two versions of a configuration file. See “Comparing different configuration files” on page 240 for more details.
Delete icon	Delete this version from the repository. You cannot delete a version that is currently active on the FortiGate unit.
Revert icon	Revert the current configuration to the selected revision. See “To revert to another configuration file:” on page 241.



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

To view the configuration settings on a FortiGate unit:

1. On the content pane with a device already selected, go to the *Configuration and Installation Status* widget, on the *Total Revisions* row, select *Revision History*.
2. Select the *ID* for the revision you want to view.

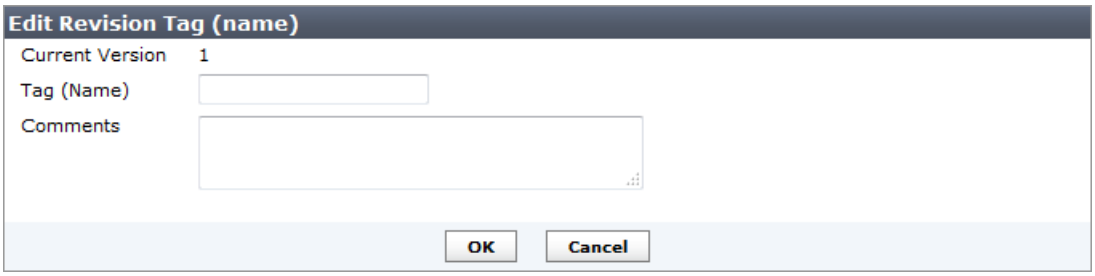
   You are automatically redirected to the View Configuration page.
3. Select *Return* when you finish viewing.

You can download the configuration settings if you want by selecting *Download* on the *View Configuration* page. For more information, see “Downloading and importing a configuration file” on page 240.

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

1. On the content pane with a device already selected, go to the *Configuration and Installation Status* widget, on the *Total Revisions* row, select *Revision History*.
2. Select the *Name* for the version you want to change.

Figure 151: Add a tag to a configuration version



3. Enter a name in the *Tag (Name)* field.
4. Optionally, enter information in the *Comments* field.
5. Select *OK*.

Downloading and importing a configuration file

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



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

To download a configuration file to a local computer:

1. On the content pane with a device already selected, go to the *Configuration and Installation Status* widget, on the *Total Revisions* row, select *Revision History*.
2. Select the *ID* for the revision you want to download.
3. Select the *Download* button.
4. Select *Regular* or *Encrypted* download type. If you select *Encrypted Download*, enter a password.
5. Select *OK*.
6. Specify a location to save the configuration file on the local computer.
7. Select *Save*.

To import a configuration file from a local computer:

1. On the content pane with a device already selected, go to the *Configuration and Installation Status* widget, on the *Total Revisions* row, select *Revision History*.
2. Select *Import*.
3. Select the location of the configuration file or choose *Browse* to locate the file.
4. If the file is encrypted, select the *File is Encrypted* check box and enter the password.
5. Select *OK*.

Comparing different configuration files

You can compare the changes or differences between two versions of a configuration file by using the *Diff* function.

The *Diff* function behaves differently under certain circumstances.

For example, when a device is first added to the FortiManager system, the FortiManager system gets the configuration file directly from the FortiGate unit and stores it as is. This configuration file is version/ID 1.

If you make changes to the device configuration on *Device Manager* tab and select Commit, the new configuration file will be saved as version/ID 2. If you use the *Diff* icon to view the changes/differences between version/ID 1 and version/ID 2, you will be shown more changes than you have made.

This happens because the items in the file version/ID 1 are ordered as they are on the FortiGate unit. Configurations of version/ID 2 are sequenced differently when they are edited and committed in the *Device Manager*. Therefore, when you compare version/ID 1 and version/ID 2, the *Diff* function sees every item in the configuration file as changed.

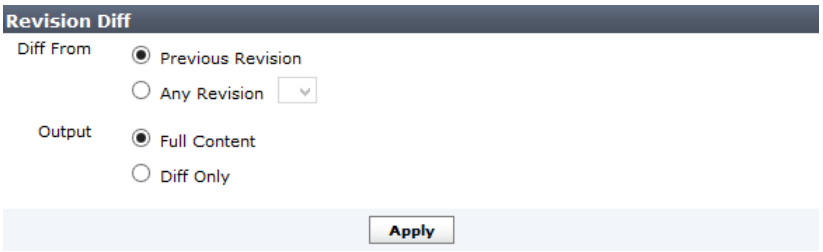
If you take version/ID 2, change an item and commit it, the tag is changed to version/ID 3. If you use *Diff* with version/ID 2 and version/ID 3, only the changes that you made will be shown. This is because version/ID 2 and version/ID 3 have both been sequenced in the same way in the *Device Manager*.

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

To compare different configuration files:

1. On the content pane with a device already selected, go to the *Configuration and Installation Status* widget, on the *Total Revisions* row, select *Revision History*.
2. On the *Total Revisions* row, select the *Revision Diff* icon, .

Figure 152: Revision *diff* dialog box



3. Select either the previous version or specify a different configuration version to compare in *Diff From*.
4. Select whether to display the full configuration file (*Full Content*) or only the differences (*Diff Only*) in *Output*.

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

   The configuration differences are displayed in colored highlights:

To revert to another configuration file:

1. On the content pane with a device already selected, go to the *Configuration and Installation Status* widget, on the *Total Revisions* row, select *Revision History*.
2. Select the *Revert* icon, , for the revision you want to revert to.
3. Select *OK*.

Advanced Features

This chapter includes:

- Scripting
- Configuring web portals



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

Script and Web Portal must be configured to be displayed to be accessible as described in this chapter. Go to *System Settings* > *Admin* > *Admin Settings* and select *Show Script* and *Show Web Portal* from the *Display Options on GUI* section to make them visible in the Web-based Manager. For more information, see "Administrator settings" on page 105.

Scripting

FortiManager scripts enable you to create, execute, and view the results of scripts executed on FortiGate devices, policy packages, the ADOM database, the global policy package, or the DB. Scripts can also be filtered based on different device information, such as OS type and platform.

At least one FortiGate device must be configured on the FortiManager system for you to be able to use scripts.



Any scripts that are run on the global database must use complete commands. For example, if the full command is `config system global`, do not use `conf sys glob`.

Scripts can be written in one of two formats:

- A sequence of FortiGate CLI commands, as you would type them at the command line. A comment line starts with the number sign (#). A comment line will not be executed.
- TCL scripting commands to provide more functionality to your scripts including global variables and decision structures.

When writing your scripts, it is generally easier to write them in a context-sensitive editor, and then cut and paste them into the script editor on your FortiManager system. This can help avoid syntax errors and can reduce the amount of troubleshooting required for your scripts.

For information about scripting commands, see the *FortiGate CLI reference*.

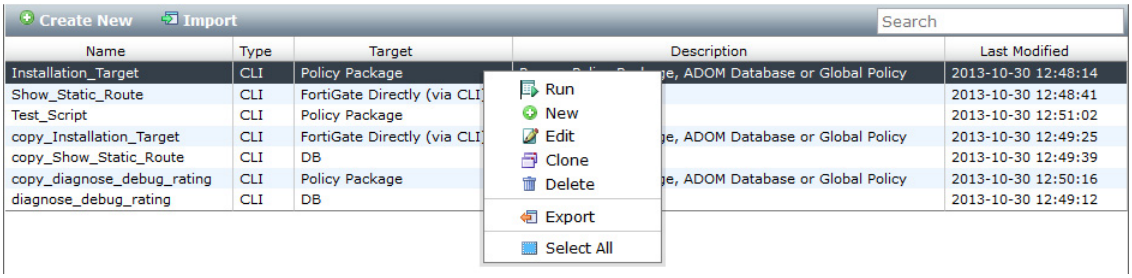


Before using scripts, ensure the `console-output` function has been set to `standard` in the FortiGate CLI. Otherwise, scripts and other output longer than a screen in length will not execute or display correctly.

Configuring scripts

To configure, import, export, or run scripts, go to the *Device Manager* tab, expand an ADOM view in the tree menu, and then select *Script* > *Script*. The script list for the selected ADOM will be displayed.

Figure 153: Script list



The following information and options are available:

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

Target	The override script target. One of the following: • FortiGate Directly (via CLI): Run on FortiGate Directly (via CLI) • Policy Package: Run on Policy Package, ADOM Database, or Global Policy • DB: Run on DB
Description	The user-defined script description.
Last Modified	The date and time that the script was last modified.

Run a script

To run a script:

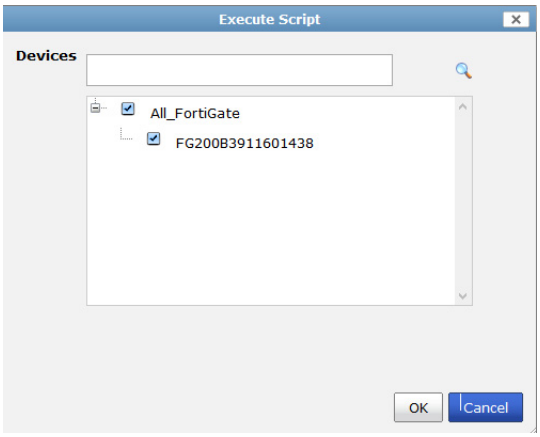
1. Browse to the ADOM script list for the ADOM that contains the script you would like to run.
2. Select the script, then right-click and select *Run* from the pop-up menu.

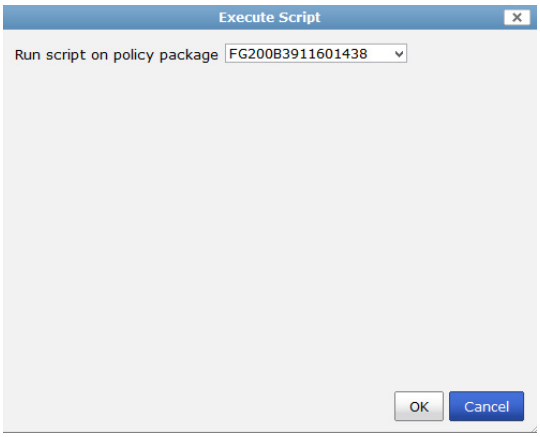


Scripts can also be re-run from the script execution history by selecting the run button, . See "Script history" on page 248 for information.

The *Execute Script* dialog box will open. This dialog box will vary depending on the script target. You will either be able to select a device or devices (left image below), or a policy package (right image). See "Override Script Target" on page 246 for more information.

Figure 154: Execute script dialog boxes





3. Select *OK* to run the script.

   The *Run Script* dialog box will open, showing the progress of the operation and providing information on its success or failure.
4. Selecting the *Details* option will expand the dialog box to show the details table, with details of the success or failure of the script.

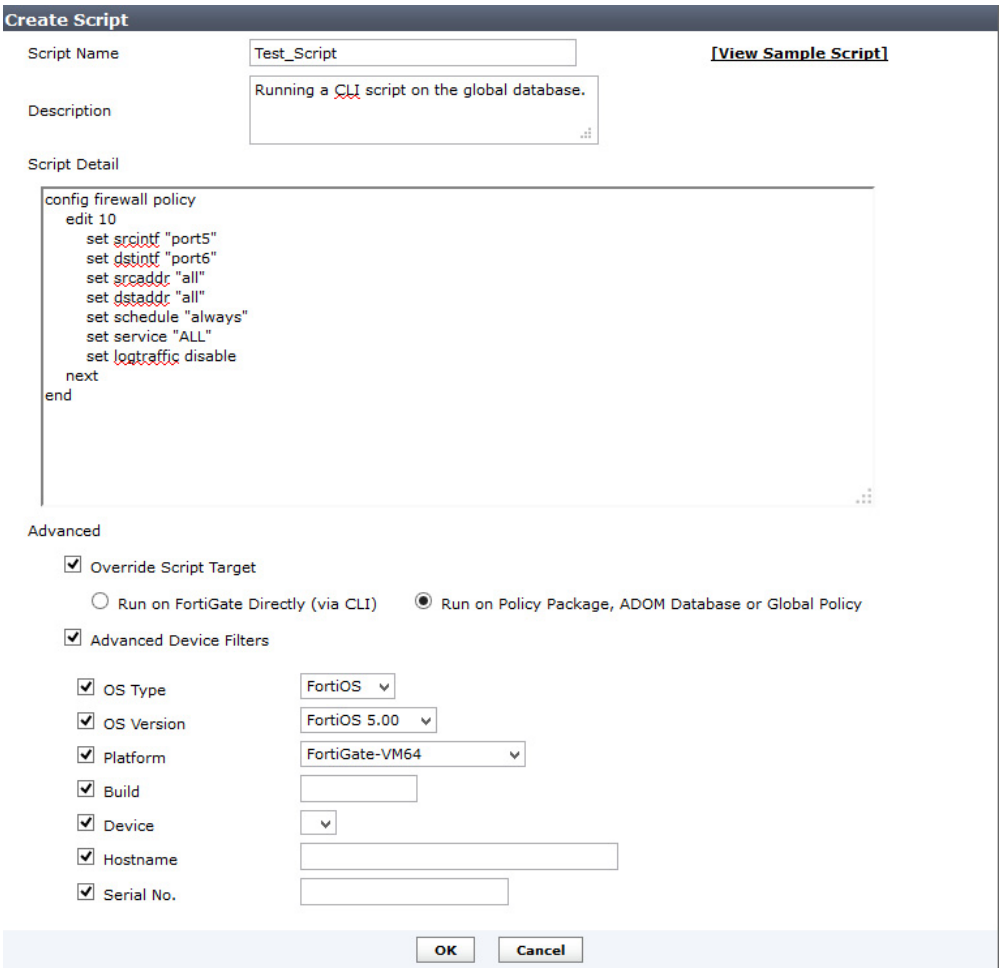
   Under the *History* column in the details table, you can select the *History* icon to open the script history for that device, and the *View Script Execution History* icon to view the script execution history for that device.
5. Close the *Run Script* dialog box when finished.

Add a script

To add a script to an ADOM:

1. Browse to the ADOM script list for the ADOM in which you will be creating the script.
2. Select *Create New*, or right-click anywhere in the script list and select *New* from the pop-up menu, to open the *Create Script* dialog box.

Figure 155: Create a new script



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

Script Name	Enter a name for the script.
View Sample Script	This option is not in use.
Description	Optionally, enter a description of your script.
Script Detail	Enter the script itself, either manually using a keyboard, or by copying and pasting from another editor.

Override Script Target	Select to change the script target. This settings will affect the options presented when you go to run a script. The options include: • *Run on FortiGate Directly (via CLI)* • *Run on Policy Package, ADOM Database or Global Policy* • *Run on DB* (default when *Override Script Target* is not selected). *Note:* The *Run on DB* option is available when editing an existing script.
Advanced Device Filter	Select to adjust the advanced filters for the script. The options include: • *OS Type* (select from the drop-down list) • *OS Version* (select from the drop-down list) • *Platform* (select from the drop-down list) • *Build* • *Device* (select from the drop-down list) • *Hostname* • *Serial No.*

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

Edit a script

All of the same options are available when editing a script as when creating a new script, except the name of the script cannot be changed.

To edit a script, from the script list of the selected ADOM, either double click on the name of the script, or right-click on the script name and select *Edit* from the pop-up menu. The *Edit Script* dialog box will open, allowing you to edit the script and its settings.

Clone a script

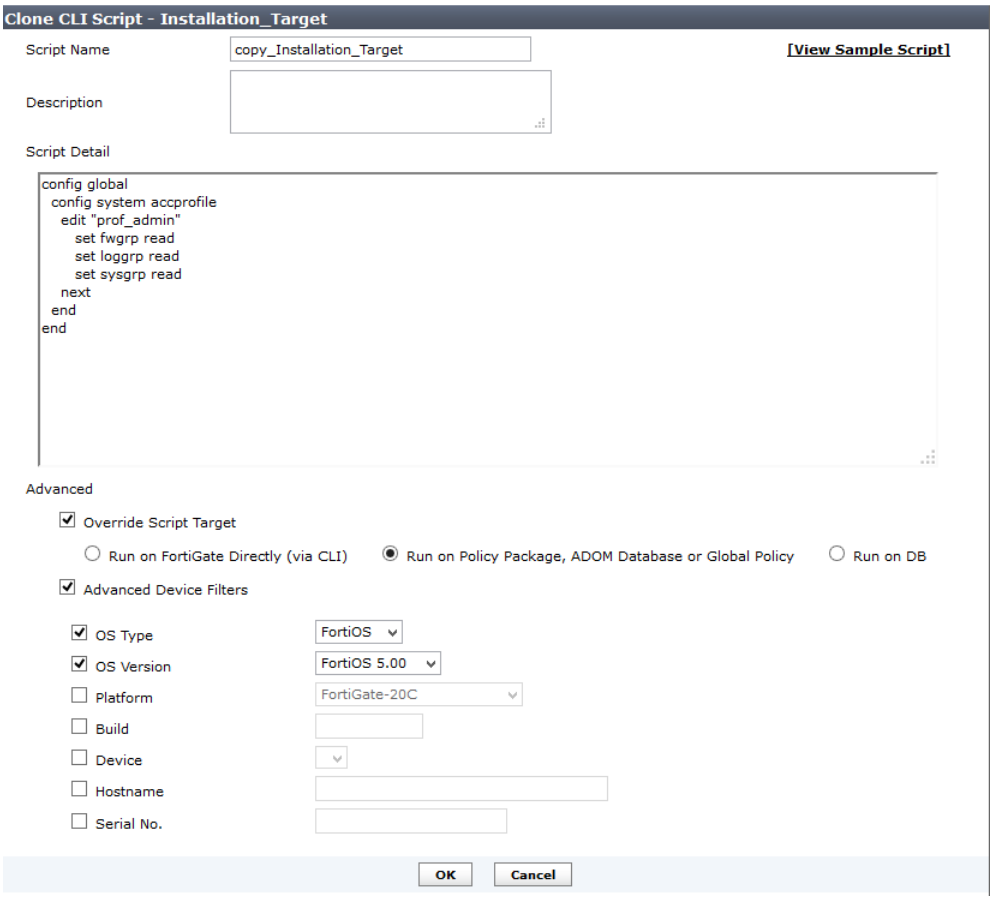
Cloning a script is useful when multiple scripts that are very similar.

To clone a script:

1. Browse to the ADOM script list for the ADOM with the script you would like to clone.
2. Select the script that you will be cloning, then right-click and select *Clone* from the menu.

   The *Clone Script* dialog box will open, showing the exact same information as the original, except *copy_* is appended to the script name and the option to *Run on DB* is available in the *Advanced* section.

Figure 156: Clone script dialog box



3. Edit the script and its settings as needed and select *OK* to create the clone.

Delete a script

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

Export a script

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

To export a script:

1. Browse to the ADOM script list for the ADOM with the script you would like to export.
2. Select the script that you will be exporting, then right-click and select *Export* from the pop-up menu.
3. If prompted by your web browser, select a location to where save the file, or open the file without saving, then select *OK*.

Import a script

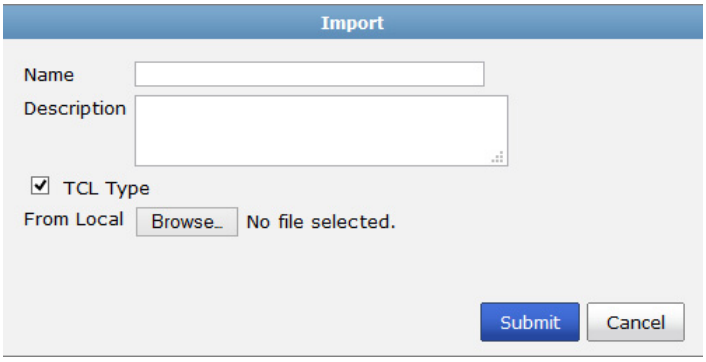
Scripts can be imported as text files from your local computer.

To import a script:

1. Browse to the ADOM script list for the ADOM you will be importing the script to.
2. Select *Import* from the toolbar.

   The Import dialog box opens.

   Figure 157: Import script dialog box



3. Enter a name and description for the script you are importing.
4. Select *TCL Type* if the script you are importing is a TCL script.
5. Select *Browse* and locate the file to be imported on your local computer.
6. Select *Submit* to import the script.

   If the script cannot be read, due to an incorrect file type or other issue, an error message will be displayed and the import process will be cancelled.

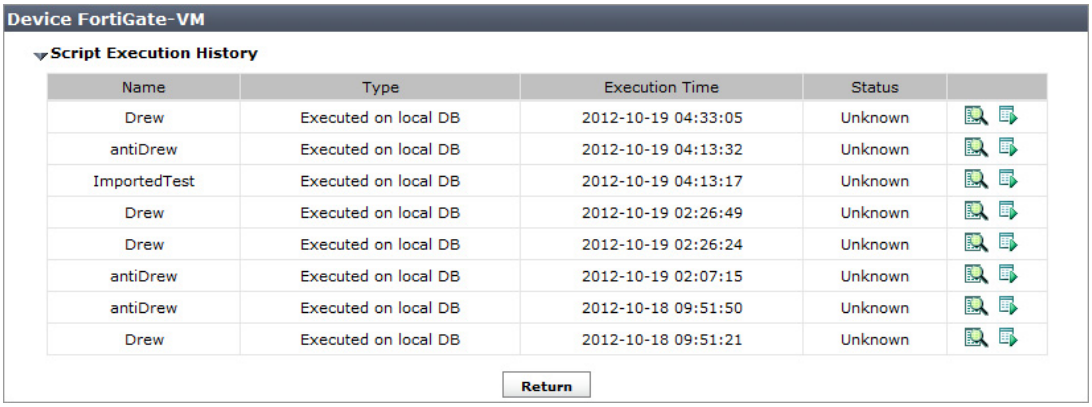
Script history

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

To view the script execution history:

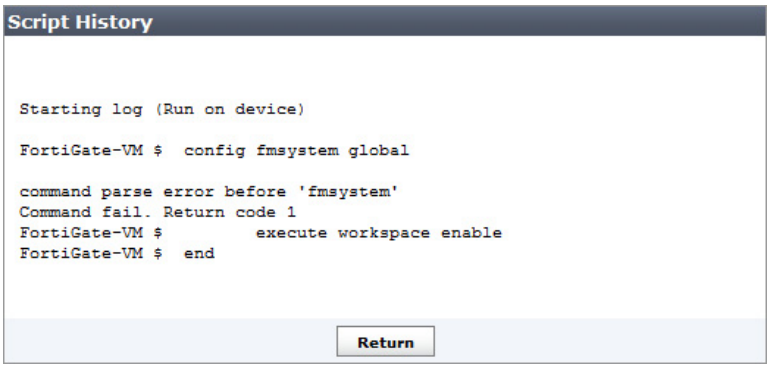
1. In *Device Manager*, locate the device whose script history you want to view.
2. In the lower content pane, select *Dashboard*, and find the *Configuration and Installation Status widget*.
3. Select *Configure* in the *Script Status* field of the widget to open the *Script Execution History table*.

Figure 158: Script execution history table



4. To view the script history for a specific script, select the *Browse* icon, , in the far right column of the table to open the *Script History* dialog box.

Figure 159: Script history dialog box.



5. To re-run a script, select the Run script now icon in the far right column of the table.
   The script is re-run. See “Run a script” on page 244 for more information.
6. Select *Return* to return to the device dashboard.

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 255.

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 255.

CLI script samples

There are two types of CLI scripts. The first type is getting information from your FortiGate device. The second type is changing information on your FortiGate device.

Getting information remotely is one of the main purposes of your FortiManager system, and CLI scripts allow you to access any information on your FortiGate devices. Getting information typically involves only one line of script as the following scripts show.

To view interface information for port1:	
Script	`show system interface port1`

Output	`config system interface`
	`  edit "port1"`
	`  set vdom "root"`
	`  set ip 172.20.120.148 255.255.255.0`
	`  set allowaccess ping https ssh`
	`  set type physical`
	`  next`
	`end`

Variations	Remove the interface name to see a list that includes all the interfaces on the FortiGate device including virtual interfaces such as VLANs.
Note	This script does not work when run on a policy package.

If the above script is used to be run on the FortiGate Directly (via CLI) or run on device database on a FortiGate has the VDOM enabled. The script will have be modified to the following:

```
config global
  show system interface port1
end
```

Since running on device database does not yield any useful information.

View the log of script running on device: FortiGate-VM64-70

```
------- Executing time: 2013-10-15 13:27:32 ------
Starting log (Run on database)
config global
end
Running script on DB success
------- The end of log ----------
```

The script should be run on the FortiGate Directly (via CLI).

View the log of script running on device: FortiGate-VM64-70

```
------- Executing time: 2013-10-15 13:52:02 ------
Starting log (Run on device)
FortiGate-VM64 $  config global
FortiGate-VM64 (global) $    show system interface port1
config system interface
    edit "port1"
        set vdom "root"
        set ip 10.2.66.181 255.255.0.0
       set allowaccess ping https ssh snmp http telnet fgfm
     auto-ipsec radius-acct probe-response capwap
        set type physical
        set snmp-index 1
    next
end
FortiGate-VM64 (global) $  end
------- The end of log ----------
```

To view the entries in the static routing table. To get any useful information, the script has to be re-written for the following if the VDOM is enabled for FortiGate and has to be run on the FortiGate Directly (via CLI).

```
config vdom
  edit root
    show route static
  next
end
```

Here is a sample run of the above script running on the FortiGate Directly (via CLI).

View the log of script running on device: FortiGate-VM64-70

```
------- Executing time: 2013-10-15 14:24:10 ------
Starting log (Run on device)
FortiGate-VM64 $  config vdom
FortiGate-VM64 (vdom) $    edit root
current vf=root:0
FortiGate-VM64 (root) $      show route static
config router static
    edit 1
        set device "port1"
        set gateway 10.2.0.250
    next
end
FortiGate-VM64 (root) $    next
FortiGate-VM64 (vdom) $  end
------- The end of log ----------
```

To view the entries in the static routing table:

Script

```
show route static
```

Output

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

Variations none

To view information about all the configured FDN servers on this device:

Script

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

Output

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

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

Variations

Output for this script will vary based on the state of the FortiGate device. The 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 global
  config system accprofile
    edit "policy_admin"
      set fwgrp read
      set loggrp read
      set sysgrp read
    next
  end
end
```

Output

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

Variations

This profile is read-only to allow a policy administrator to monitor this device's configuration and traffic.

Variations may include enabling other areas as read-only or write 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 vdom
edit "root"
  config firewall policy
    edit 10
      set srcintf "port5"
      set dstintf "port6"
      set srcaddr "all"
      set dstaddr "all"
      set status disable
      set schedule "always"
      set service "ALL"
      set logtraffic disable
  next
```

```
end
```

- Running a CLI script on the global database

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

Error Messages

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

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

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

Troubleshooting Tips

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

- Check the script output. Generally the error messages displayed here will help you locate and fix the problem.
- See the *FortiGate CLI Reference* for more information on all CLI commands.
- There is a limit to the number of scripts allowed on the FortiManager unit. Try removing an old script before trying to save your current one.
- As mentioned at the start of this chapter, ensure the `console more` command is disabled on the FortiGate devices where scripts execute. Otherwise a condition may occur where both the FortiGate device and the FortiManager system are waiting for each other to respond until they timeout.
- There should be no punctuation at the start or end of the lines.
- Only whitespace is allowed on the same line as the command. This is useful in lining up `end` and `next` commands for quick and easy debugging of the script.

- Keep your scripts short. They are easier to troubleshoot and it gives you more flexibility. You can easily execute a number of scripts after each other.
- Use full command names. For example instead of “set host test” use “set hostname test”. This is required for any scripts that are to be run on the global database.
- Use the number sign (#) to comment out a line you suspect contains an error.

TCL scripts

TCL is a 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

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 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
puts [exec "# This is an example TCL script to get the system status of
     the FortiGate\n" "# " 15 ]
  set input [exec "get system status\n" "# " 15 ]
# puts $input
  set linelist [split $input \n]
# puts $linelist
foreach line $linelist {
  if {![regexp {([^:]+):(.*)} $line dummy key value]} continue
    switch -regexp -- $key {
    Version {
    regexp {FortiGate-([^ ]+) ([^,]+),build([\d]+),.*} $value dummy
         a(platform) a(version) a(build)
  }
Serial-Number {
  set a(serial-number) [string trim $value]
}
  Hostname {
    set a(hostname) [string trim $value]
    }      }
  }
}
get_sys_status status
puts "This machine is a $status(platform) platform."
puts "It is running version $status(version) of FortiOS."
puts "The firmware is build# $status(build)."
puts "S/N: $status(serial-number)"
puts "This machine is called $status(hostname)"
```

Output

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

FortiGate-VM64 #

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

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

Variations

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

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

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

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

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

In analyzing this script:

- line 1 is the required #! to indicate this is a TCL script
- lines 2-3 open the procedure declaration
- lines 4-5 puts the output from the CLI command into a TCL variable as a string, and breaks it up at each return character into an array of smaller strings
- line 6 starts a loop to go through the array of strings
- line 7 loops if the array element is punctuation or continues if its text
- line 8 takes the output of line 7's regular expression command and based on a match, performs one of the actions listed in lines 9 through 17
- lines 9-11 if regular expression matches 'Version' then parse the text and store values for the platform, version, and build number in the named array elements
- line 12-14 if regular expression matches 'Serial-Number' then store the value in an array element named that after trimming the string down to text only
- lines 15-17 is similar to line 12 except the regular expression is matched against 'Hostname'
- line 17-19 close the switch decision statement, the for each loop, and the procedure
- line 20 calls the procedure with an array name of status
- lines 21-25 output the information stored in the status array

TCL loops

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

To create 10 users from usr0001 to usr0010:

Script

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

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

Output

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

------- Executing time: 2013-10-16 15:27:18 ------
Starting log (Run on device)
config vdom
FortiGate-VM64 (vdom) #
edit root
current vf=root:0
FortiGate-VM64 (root) #
config user local
FortiGate-VM64 (local) #
Adding user: usr0001
edit usr0001
new entry 'usr0001' added
FortiGate-VM64 (usr0001) #
set status enable
FortiGate-VM64 (usr0001) #
set type password
```

```
FortiGate-VM64 (usr0001) #
next

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

Variations

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

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

In analyzing this script:

- line 1 is the required #! to indicate this is a TCL script
- lines 2-4 open CLI command wrapper procedure
- line 5 declares the number of users to create
- line 6 gets the FortiGate ready for entering local users
- line 7 opens the for loop that will loop ten times
- line 8 sets the 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

```
#!
# need to define procedure do_cmd
# the second parameter of exec should be "# "
# If split one command to multiple lines use "\" to continue
```

```
proc do_cmd {cmd} {
  puts [exec "$cmd\n" "# "]
}
foreach line [split [exec "show firewall policy\n" "# "] \n] {
  if {[regexp {edit[ ]+([0-9]+)} $line match policyid]} {
    continue
  } elseif {[regexp {set[ ]+(\w+)[ ]+(.*)\r} $line match key value]} {
    lappend fw_policy($policyid) "$key $value"
  }
}
do_cmd "config firewall policy"
foreach policyid [array names fw_policy] {
  if {[lsearch $fw_policy($policyid){diffservcode_forward 000011}] == -1} {
    do_cmd "edit $policyid"
    do_cmd "set diffserv-forward enable"
    do_cmd "set diffservcode-forward 000011"
    do_cmd "next"
  }
}
do_cmd "end"
```

Variations

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

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

In analyzing this script:

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

Additional TCL Scripts

To get and display state information about the FortiGate device:

Script

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

Output

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

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

CPU states: 0% user 0% system 0% nice 100% idle
CPU0 states: 0% user 0% system 0% nice 100% idle
CPU1 states: 0% user 0% system 0% nice 100% idle
Memory states: 73% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes, 0 kbps
     in 30 minutes
Average sessions: 1 sessions in 1 minute, 2 sessions in 10 minutes, 2
     sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0
     sessions per second in last 10 minutes, 0 sessions per second in
     last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 6 days,  1 hours,  34 minutes

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


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

To configure common global settings:

Script

```
#!
#Run on FortiOS v5.00
#This script will configure common global, user group and ntp settings
#if you do not want to set a parameter, comment the
#corresponding set command
#if you want to reset a parameter to it's default
#value, set it an empty string
puts [exec "# This is an example TCL script to configure global, user
     group and ntp setting of FortiGate\n" "# " 15 ]

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

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

```
}
fgt_cmd "end"
fgt_cmd "end"
#config system user group---end

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

Output

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

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

To configure syslogd settings and filters:

Script

```
#!
#Run on FortiOS v5.00
#This script will configure log syslogd setting and
#filter
#key-value pairs for 'config log syslogd setting', no
#value means default value.
  set setting_list {{status enable} {csv enable}
{facility alert} {port} {server 1.1.1.2}}
#key-value pairs for 'config log syslogd filter', no
#value means default value.
puts [exec "# This is an example TCL script to configure log syslogd
     setting and filter setting of FortiGate\n" "# " 15 ]
  set filter_list {{attack enable} {email enable} {severity} {traffic
       enable} {virus disable}
{web enable}}
#set the number of syslogd server, "", "2" or "3"
  set syslogd_no "2"
#procedure to execute FortiGate CLI command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# "]
}
#procedure to set a series of key-value pairs
proc set_kv kv_list {
foreach kv $kv_list {
  set len [llength $kv]
if {$len == 0} {
continue
} elseif {$len == 1} {
fgt_cmd "unset [lindex $kv 0]"
} else {
fgt_cmd "set [lindex $kv 0] [lindex $kv 1]"
}
}
}
#configure log syslogd setting---begin
fgt_cmd "config global"
fgt_cmd "config log syslogd$syslogd_no setting"
  set_kv $setting_list
fgt_cmd "end"
#configure log syslogd setting---end
#configure log syslogd filter---begin
fgt_cmd "config log syslogd$syslogd_no filter"
  set_kv $filter_list
fgt_cmd "end"
#configure log syslogd filter---end
```

Output

```
Starting log (Run on device)

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

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

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

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 enc-algorithm high
#localid will be set as the hostname automatically
#later
puts [exec "# This is an example TCL script to configure the FortiGate
     to communicate with a FortiAnalyzer\n" "# " 15 ]
  set server 1.1.1.1
#for fortianalyzer, fortianalyzer2 or
#fortianalyzer3, enter the corresponding value "",
#"2", "3"
  set faz_no ""
#keys used for 'config system fortianalyzer', if you
#do not want to change the value of a key, do not put
#it in the list
  set key_list {status enc-algorithm localid server }
##procedure to get system status from a FortiGate
proc get_sys_status aname {
```

```
  upvar $aname a
  set input [split [exec "get system status\n" "# "]  \n]
  foreach line $input {
    if {![regexp {([^:]+):(.*)} $line dummy key value]} continue
    set a([string trim $key]) [string trim $value]
  }
}
#procedure to execute FortiGate command
proc fgt_cmd cmd {
  puts -nonewline [exec "$cmd\n" "# "]
}
#set the localid as the FortiGate's hostname
get_sys_status sys_status
set localid $sys_status(Hostname)
#config system fortianalyzer---begin
fgt_cmd "config global"
fgt_cmd "config log fortianalyzer$faz_no setting"
foreach key $key_list {
  if [info exists $key] {
     fgt_cmd "set $key [set $key]"
   } else {
      fgt_cmd "unset $key"
   }
}
fgt_cmd "end"
fgt_cmd "end"
#config system fortianalyzer---end
```

Output

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

To create custom IPS signatures and them to a custom group:

Script

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

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

Output

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

Variations

None.

TCL file IO

You can write to and read from files using TCL scripts. For security reasons there is only one directory on the FortiManager where scripts can access files. For this reason, there is no reason to include the directory in the 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 10MB of diskspace allocated for TCL scripts. An error will be reported if this size is exceeded.

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

To write to a file:	

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

To read from a file	

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

Output	`Hello, world!`

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

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

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

Both scripts close the file before they exit.

Troubleshooting Tips

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

- Make sure the commands you are trying to execute are valid for the version of FortiOS running on your target FortiGate device.
- You should always use braces when evaluating code that may contain user input, to avoid possible security breaches. To illustrate the danger, consider this interactive session:

```
% set userinput {[puts DANGER!]}
[puts DANGER!]
% expr $userinput == 1
DANGER!
0
% expr {$userinput == 1}
0
```

In the first example, the code contained in the user-supplied input is evaluated, whereas in the second the braces prevent this potential danger. As a general rule, always surround expressions with braces, whether using expr directly or some other command that takes an expression.

- A number that includes a leading zero or zeros, such as 0500 or 0011, is interpreted as an octal number, not a decimal number. So 0500 is actually 320 in decimal, and 0011 is 9 in decimal.
- There is a limit to the number of scripts allowed on the FortiManager unit. Try removing an old script before trying to save your current one.
- Using the TCL command “catch” you can add custom error messages in your script to alert you to problems during the script execution. When catch encounters an error it will return 1, but if there is no error it will return 0. For example:

```
if { [catch {open $someFile w} fid] } {
    puts stderr "Could not open $someFile for writing\n$fid"
    exit 1 ;# error opening the file!
  } else {
# put the rest of your script here
  }
```

Configuring web portals

The web portal enables MSSP customers to manage their own SSL VPN user list, web filtering, URL filters, and categories. If configured, customers can also view the firewall policies on their FortiGate devices or VDOM.

You create a portal profile and include its content and appearance. You can then create more profiles if customers have differing needs. The portal is composed of selected configuration and monitoring widgets, on one or more pages, to provide the specific functionality that the administrators need to monitor their network security. You can also customize the web portal with a logo and select the colors and page layouts for your business, or match the customer’s corporate look. With FortiManager, you define each customer/administrator as a portal user, assigned to a specific portal profile.

Using FortiManager, you can maintain a number of FortiGate units and/or VDOMs for a large number of clients. These clients may also want to monitor and maintain their own firewall policies and traffic.

Customers access the web portal through the IP or URL of the FortiManager system. They log in the same way as the FortiManager administrator, using their own user name and password, created by the FortiManager administrator. Once logged in, the customer is directed to their assigned web portal. The customer does not have access to the FortiManager Web-based Manager.

To create a web portal for customers to access, you need to first create a portal profile. A web portal is similar to a group. Once set up, portal users, or administrators, can be added to the portal.

After creating a web portal, you can configure it to add components that the user or administrator can review and modify as required. You can return at anytime to add and remove components from the portal. It is a good idea to discuss with your users which components they would like to see on their portal. Provide them a list of what options they have, and allow them to select from the list.

The web portal can also be customized to a selection of color schemes, and you can add a user's logo to make the portal to fit the customer's corporate look. Users are not able to modify the layout or look of the web portal, although they can add and modify the content of some of the components. For example, they can add SSL VPN users, modify URL filter lists, and add text notes. If they require changes to the components (adding or removing) or the layout of the components on the portal page, they will need to contact you.

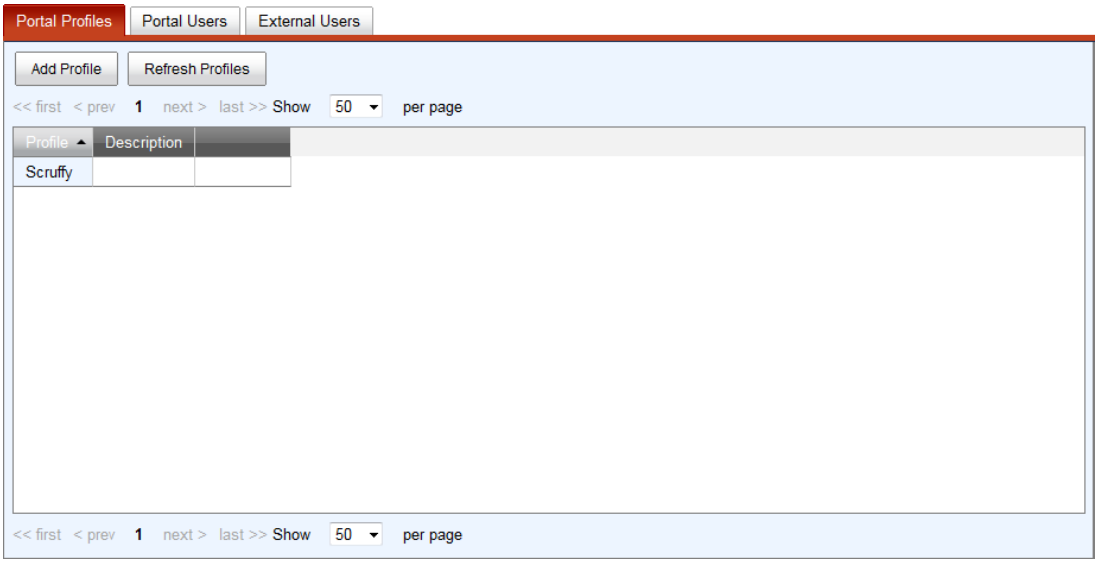
Creating a web portal

Before creating a web portal, ensure you have an ADOM configured and any VDOMs enabled and configured. You may also want to discuss with your user as to what components they want or required for their portal.

To create a web portal profile:

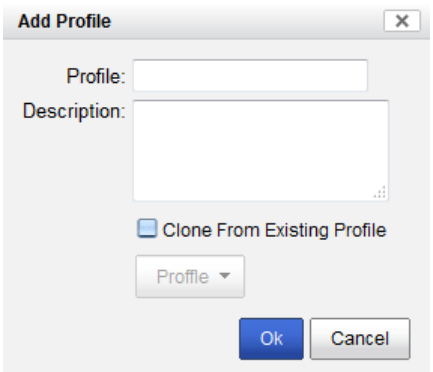
1. In the device manager tab, select the ADOM in which the web portal will be created.
2. Select *Web Portal*.

Figure 160: Web portal window



3. Select *Add Profile* to open the *Add Profile* dialog box.

Figure 161: Add profile dialog box



4. In the *Profile* field, enter a name for the profile, and optionally, enter a description in the *Description* field. The profile name can be a maximum of 35 characters and cannot contain spaces.
5. If you have already added a portal profile you can select *Clone from existing profile* to add the new profile using the settings from a previously added profile.
6. Select *OK*.

Configuring the web portal profile

With the web portal profile added, you can configure the portal with the available widgets.

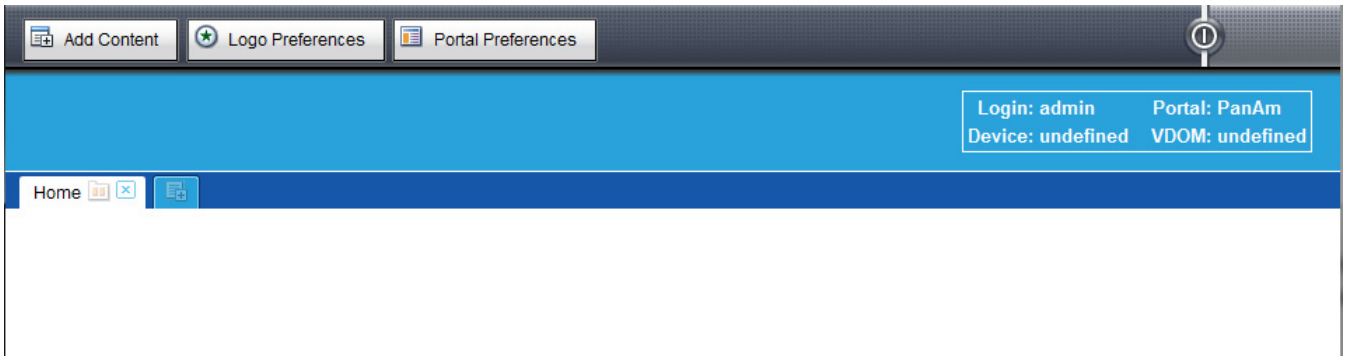
To configure the web portal profile:

1. On the web portal screen, select a profile from the list.
2. Either select the *Configure Profile* icon for the profile, or right click on the profile and select *Configure Profile* from the pop-up menu.

   The *Configure Profile* dialog box opens.
3. Select *Configure Profile*.

   The web portal design window opens in a new window or tab of the browser. You may need to allow pop ups for the FortiManager IP or URL to allow the portal design window to appear, otherwise this window will not appear.

Figure 162: Blank web portal window



Modifying the content and layout

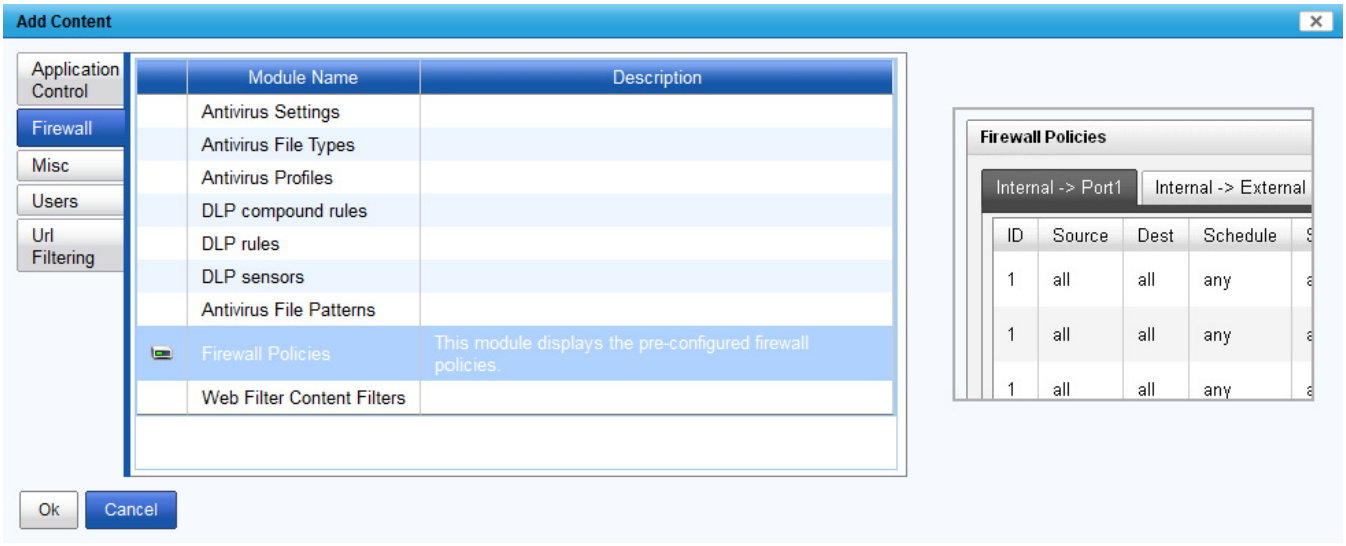
The web portal design window enables you to add content for the user's internet and firewall connection and arrange the layout of the information.

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 163: Adding web portal content



A number of content options are available. Select a tab on the left to view the available widgets. To add a particular widget, either double-click to add the content, or select a widget and select *OK*. Holding the CTRL or Shift keys on your keyboard enables you to select multiple widgets at the same time.

Once you have selected the widgets, you can move them on the page within the chosen column view.



You can change the width of the columns. When you move your cursor between the widgets, you will see a line appear, marking the column borders. Click and drag that line to the left or right to expand or contract the column width.

Many of the widgets are configurable. In the title bar of the widgets, if there is an *Edit* or *Dependencies* icon on the right further configuration can be done to the widget.



You can change the widgets vertical size by clicking and dragging the bottom of the widget

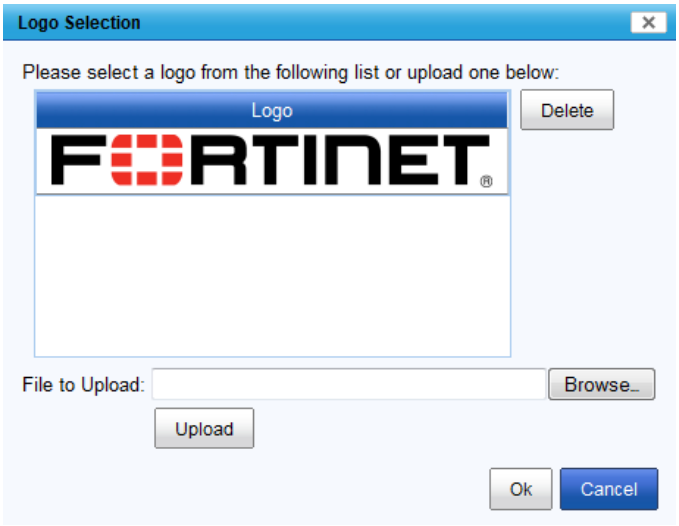
Adding a logo

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 164: Logo preferences



2. Select *Browse* and locate the desired logo on your hard disk or network volume.
3. Select *Upload*.
4. Select the uploaded logo in the logo list, and then select *OK*.

Portal preferences

You can change the colors of the display from a list of color themes. To change the colors of the web portal display, select *Portal Preferences*, select the desired color scheme from the list, and select *OK*.

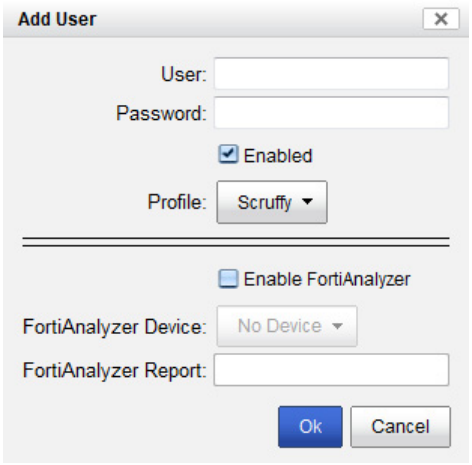
Figure 165: Portal properties window



Creating a portal user account

To create a portal user account, in the Web Portal screen of the selected ADOM, select the *Portal Users* tab, and then select *Add User*. The *Add User* dialog box will open.

Figure 166: Add user dialog box



Enter the below information and then select OK to create the new portal user.

User	Enter the name of the user who will log into the portal. The user name must be 35 or less characters.
Password	Enter the password for the user. The password must be 20 or less characters.
Enabled	Select to enable the user profile.
Profile	Select the web portal profile that this user will log into from the drop-down list.
Enable FortiAnalyzer	Select to enable a FortiAnalyzer device to use the profile.
FortiAnalyzer Device	Select a FortiAnalyzer device from the drop-down list.
FortiAnalyzer Report	Enter the name of the FortiAnalyzer report.

External users

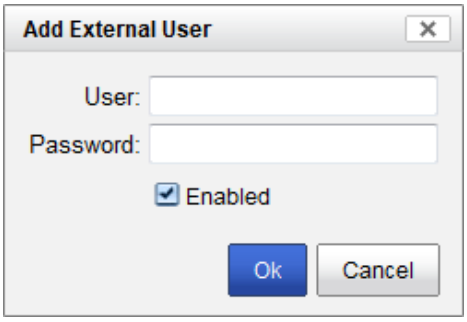
Use the *External Users* tab to add external users. This enables users to have remote access to the managing FortiManager unit from the portal FortiManager unit.

You also use external users when creating custom widgets that you can add on custom portal web pages or web portals.

To add external users:

1. In the *Web Portal* screen, select the *External Users* tab.
2. Select *Add External User*.

Figure 167: Add external user window



3. Enter the required information and select *OK*.

User	Enter a name for the external user.
Password	Enter a password for the external user.
Enabled	Select to enable the external user.

Using the web portal

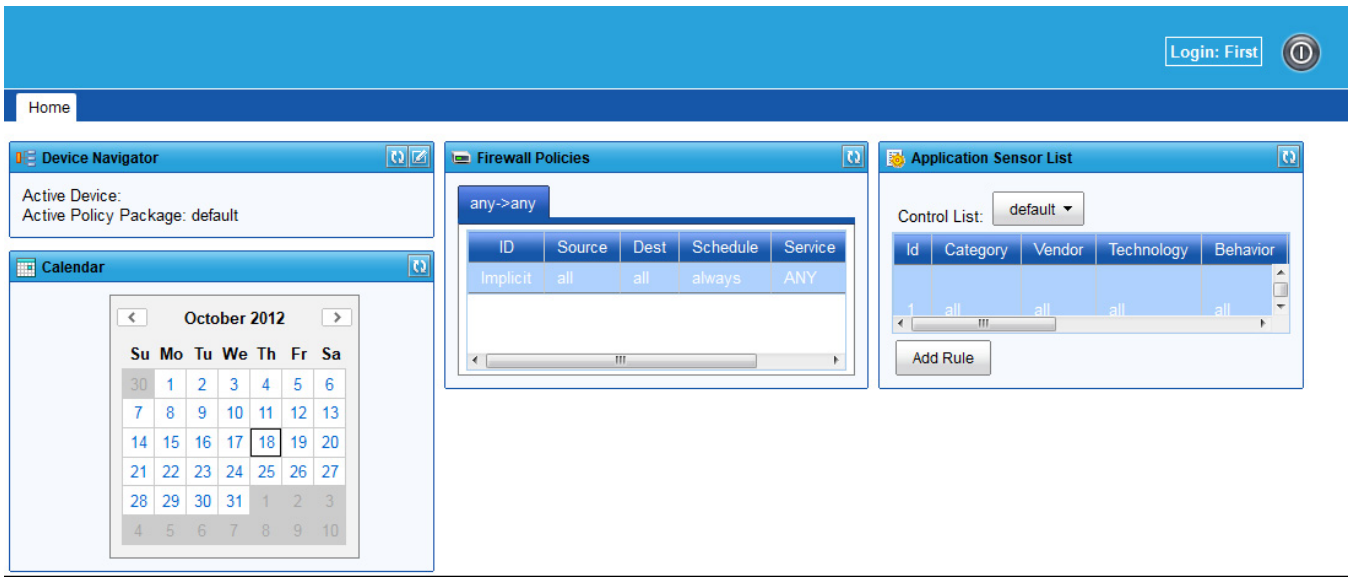
The purpose of the web portal is to enable customers, or their administrators to monitor and maintain their firewall settings.

Before the users can use the web portal you need to supply them with the URL or IP address of the FortiManager system, and their user name and password.

The user enters the FortiManager system URL or IP address into the web browser. When they get the login screen, they enter the supplied user name and password. This will log them into the portal site, displaying the colors, widgets and arrangements setup from the previous steps.

The administrator can view firewall information, maintain, and update information depending on the widgets included for the portal. The user can log out of the portal by selecting the *Logout* button in the upper right corner of the browser window.

Figure 168: Web portal

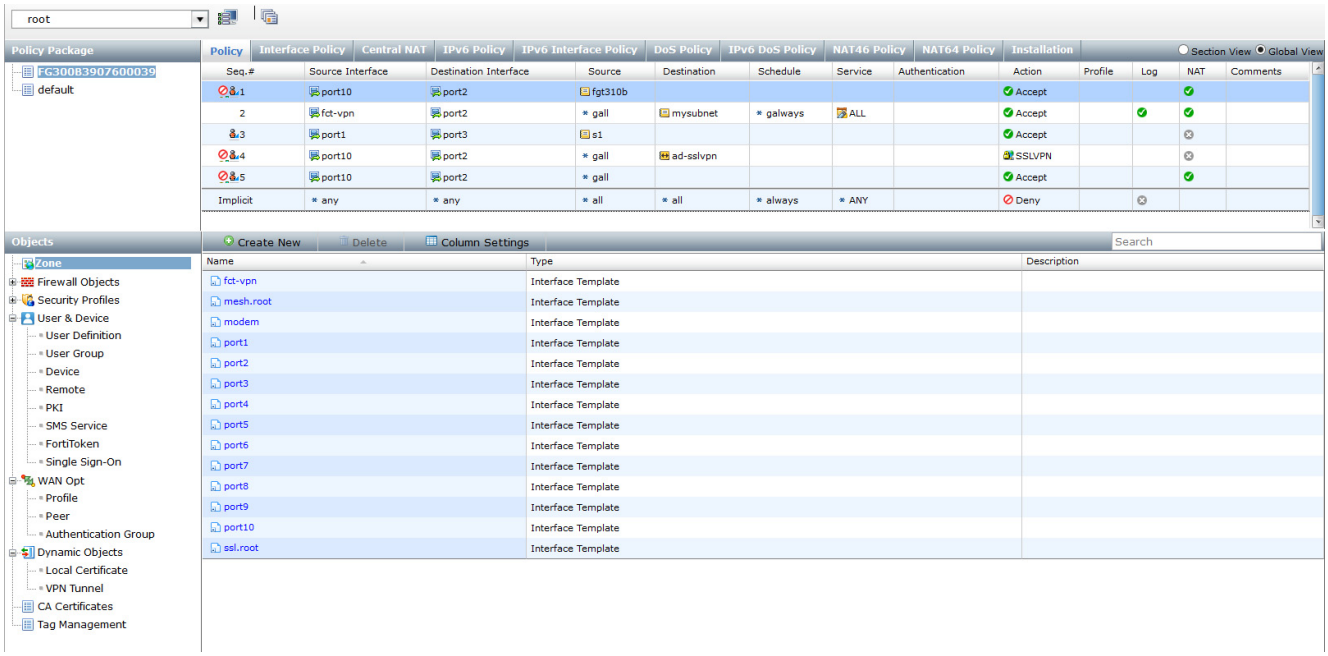


Policy & Objects

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

If the administrator account you logged on with does not have the appropriate privileges, you will not be able to edit or delete settings, or apply any changes. Instead you are limited to browsing. To modify these settings, see “Profile” on page 98.

Figure 169:ADOM Level Policy & Objects



If workspace is enabled, an ADOM must be locked before any changes can made to policy packages or objects. See “Concurrent ADOM access” on page 52 for information on enabling or disabling workspace.

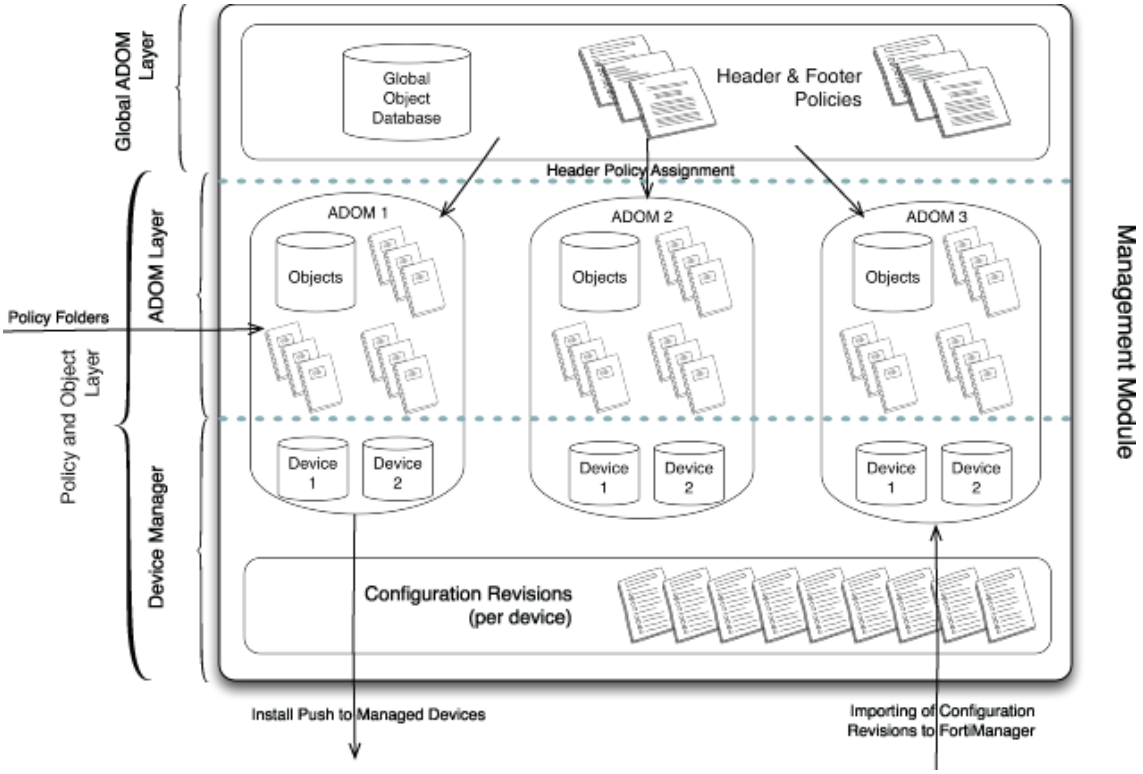
About policies

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

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

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

Figure 170: Management model



Policy theory

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

Security policies are instructions that units use to decide connection acceptance and packet processing for traffic attempting to pass through. When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a security policy matching the packet.

Security policies can contain many instructions for the unit to follow when it receives matching packets. Some instructions are required, such as whether to drop or accept and process the packets, while other instructions, such as logging and authentication, are optional.

Policy instructions may include Network Address Translation (NAT), or Port Address Translation (PAT), or they can use virtual IPs or IP pools to translate source and destination IP addresses and port numbers.

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

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

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

- Policy Type and Subtype
- Incoming Interface
- Source Address
- Outgoing Interface
- Destination Address
- Schedule and time of the session's initiation
- Service and the packet's port numbers.

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

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

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

Create security policies based on traffic flow. For example, in a policy for POP3, where the email server is outside of the internal network, traffic should be from an internal interface to an external interface rather than the other way around. It is typically the user on the network requesting email content from the email server and thus the originator of the open connection is on the internal port, not the external one of the email server. This is also important to remember when viewing log messages, as the source and destination of the packets can seem backwards.

Global policy packages

Global policies and objects function in a similar fashion to local policies and objects, but are applied universally to all ADOMs and VDOMs inside your FortiManager installation. This allows users in a carrier, service provider or large enterprise to support complex installations that may require their customers to pass traffic through their own network.

For example, a carrier or host may allow customers to transit traffic through their network, but do not want their customer to have the ability to access the carrier's internal network or resources. Creating global policy header and footer packages to effectively "surround" a customer's policy packages can help maintain security.

Global policy packages must be explicitly assigned to specific ADOMs to be used. When configuring global policies, a block of space in the policy table is reserved for *Local Domain Policies*. All of the policies in an ADOM's policy table is inserted into this block when the global policy is assigned to an ADOM.

Display options for policies and objects can be configured in *System Settings* > *Admin* > *Admin Settings.*



Global policies and objects are not supported on all FortiManager platforms. Please review the products' datasheets to determine support.



A global policy license is not required to use global policy packages.

Policy workflow

An administrator will typically carry out 2 main functions with their devices through FortiManager: provisioning new devices or VDOMs on the network and managing the day-to-day operations of managed devices and VDOMs.

Provisioning new devices

There are multiple steps to provision a new device or VDOM to be managed by the FortiManager unit:

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

Day-to-day management of devices

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

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

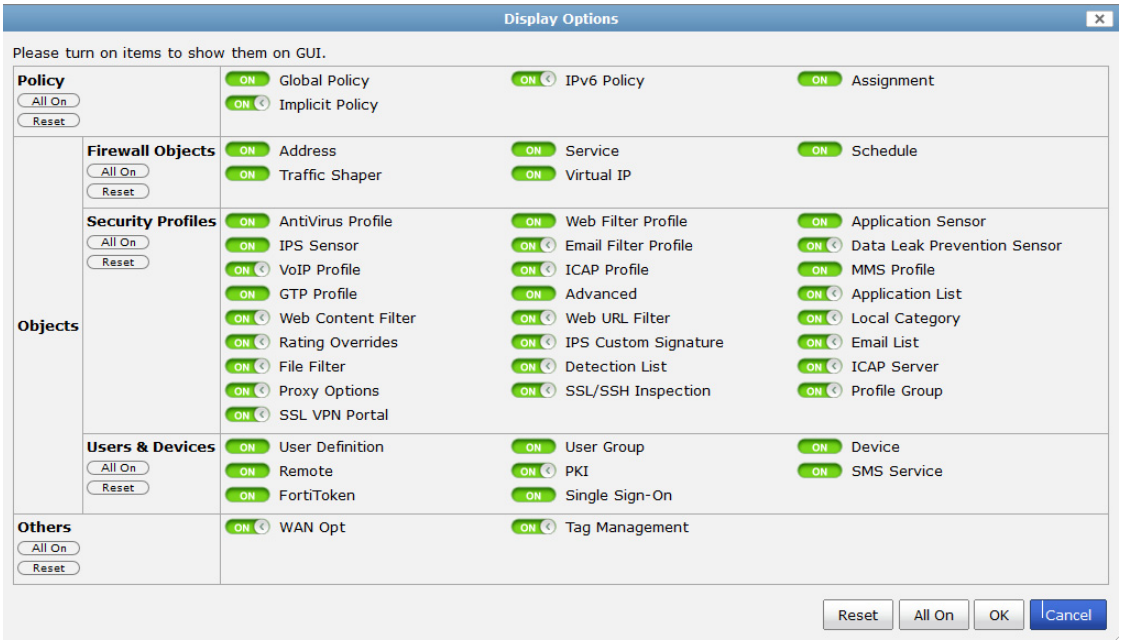
Display Options

The objects that are displayed on the Policy & Objects page can be customized by selecting the *Display Options* button, , in the toolbar. Customizations are either per ADOM or at Global level.

Figure 171:ADOM level display options



Figure 172: Global level display options



Turn the various options on or off (visible or hidden) by selecting the on/off button next to their name. Turn all of the options in a category on by selecting *All On* under the category name, or turn all of the categories on by selecting *All On* at the bottom of the window.

Once turned on, the corresponding options settings will be configurable from the appropriate location in the Policy & Objects tab.

Reset all of the options by selecting *Reset* at the bottom of the screen, or reset only the options in a category by selecting *Reset* under the category name.

Managing policy packages

Policy packages can be created and edited and then assigned to specific devices in the ADOM. Folders can be created for the policy packages to aid in the organization and management of the packages.



Not all policy and object options are enabled by default. To configure the enabled options, go to *System Settings* > *Admin* > *Admin Settings* and select your required options. See “Administrator settings” on page 105 for more information.

Lock an ADOM

If workspace is enabled, you must lock an ADOM prior to performing any management tasks on it.

To lock an ADOM:

1. Select the specific ADOM on which you will be making changes from the drop-down list in the toolbar, or select *Global*.
2. Select the lock icon next to the drop-down list to lock the selected ADOM.

   The ADOM will now be locked, allowing you to make changes to it, and preventing other administrators from making any changes, unless lock override is enabled (see "Extend workspace to entire ADOM" on page 51).

Create a new policy package or folder

To create a new policy folder:

1. Select the specific ADOM in which you are creating the policy folder from the drop-down list in the toolbar, or select *Global* to create a folder for global policy packages.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Folder* heading in the pop-up menu, select *Create New*.
4. Enter a name for the new policy folder in the dialog box and then select *OK*.

To create a new global policy package:

1. Select *Global* in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Global Policy Package* heading in the pop-up menu, select *Create New*.

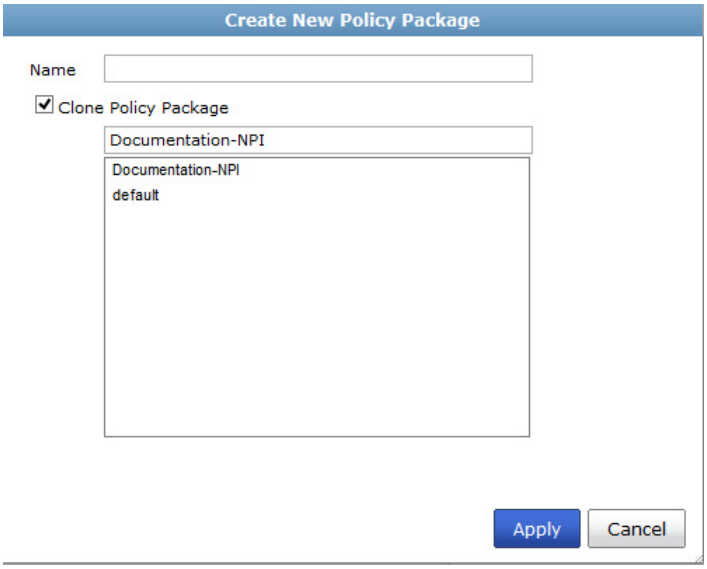
   The *Add Global Policy Package* dialog box opens.
4. Enter a name for the new global policy package in the dialog box.
5. If you are cloning a previous policy package, select *Clone Policy Package* and enter the name of the policy package you would like to clone in the resulting text field.
6. Select *OK* to add the policy package.

To create a new policy package:

1. Select the specific ADOM in which you are creating the policy package from the drop-down list in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Package* heading in the pop-up menu, select *Create New*.

   The *Create New Policy Package* dialog box opens.

Figure 173: Create new policy package



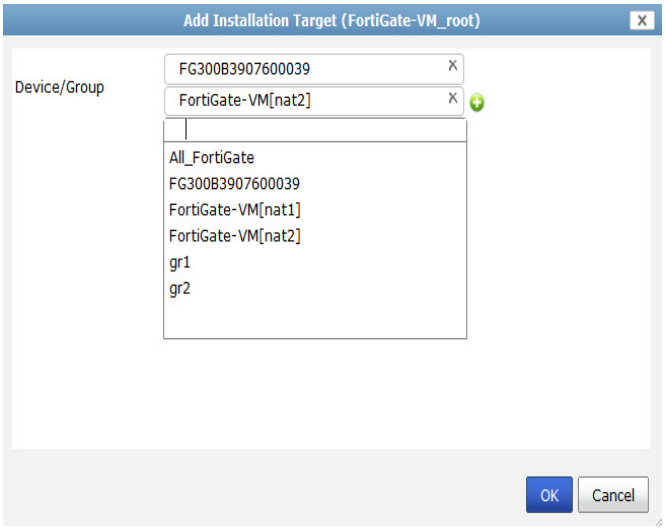
4. Configure the following settings:

Name	Enter a name for the new policy package
Clone Policy Package	If you are cloning a previous policy package, select *Clone Policy Package* and select the policy package you would like to clone from the list.

5. Select *OK* to add the policy package.
6. Select *Installation* in the Policy Package tab bar and select *Add* in the toolbar.

   The *Add Device/Group to Policy Package Installation Target* window opens.

Figure 174: Installation Targets



7. Select the devices or groups for the policy package.
8. Select *OK* to save the setting.

Remove a policy package or folder

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

Rename a policy package or folder

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

To rename a local policy package, right-click on the policy package and select *Edit*. Enter the new name (or edit the current name) in the *Name* field of the *Edit Policy Package* dialog box and select *Apply*.

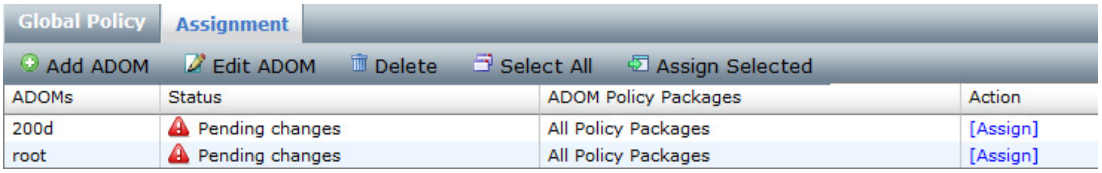
Assign a global policy package

Global policy packages can be assigned, or installed, to specific ADOMs.

To assign a global policy package:

1. Select *Global* in the toolbar and select a policy package in the *Policy Package* tree.
2. Select *Assignment* in the Policy Package tab bar to view the ADOM assignment list.

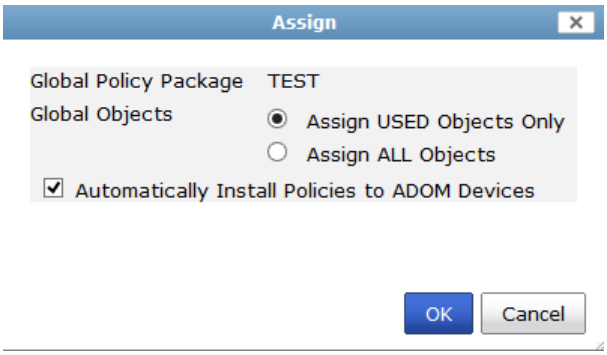
Figure 175:ADOM assignment list



3. If required, select *Add ADOM* from the content toolbar to add an ADOM to the list.
4. Select the ADOM you would like to assign from the list, or select *Select All* from the toolbar to select all of the ADOMs in the list.
5. Select *Assign Selected* from the toolbar.

   The *Assign* dialog box opens.

Figure 176: Assign dialog box



6. Select whether you want to assign only used objects or all objects, and if policies will be automatically installed to ADOM devices.
7. Select *OK* to assign the policy package to the selected ADOM or ADOMs.

Install a policy package

To install a policy package to a target device:

1. Select the specific ADOM that contains the policy package you are installing from the drop-down list in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Package* heading in the pop-up menu, select *Install*.

   The install wizard opens.
4. Follow the steps in the install wizard to install the policy package.

   For more information on the install wizard, see "Install wizard" on page 224. For more information on editing the installation targets, see "Edit the installation targets for a policy package" on page 288.

Re-install a policy package

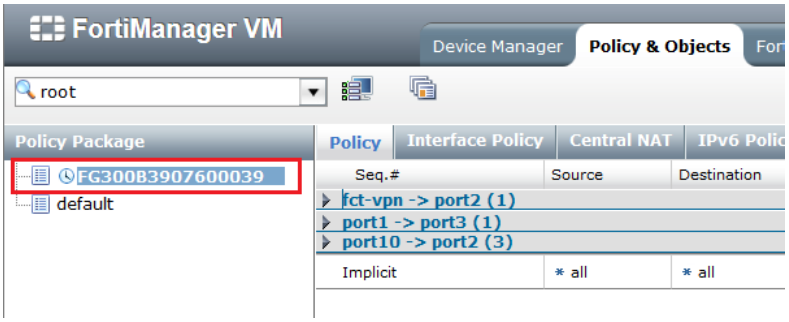
To re-install a policy package to a target device:

1. Select the specific ADOM that contains the policy package you are installing from the drop-down list in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Package* heading in the pop-up menu, select *Re-install*.
4. The policy package will be re-installed to the target device.

Schedule a policy package install

In FortiManager v5.0 Patch Release 5 or later, you can create, edit, and delete install schedules for policy packages. The Schedule Install menu has been added to the *Policy Package* right-click menu. You can specify the date and time to install the latest policy package changes. When a scheduled install has been configured and is active, an icon is displayed beside the policy package name. You can click this icon to edit or cancel the schedule. Once the scheduled install has completed, the icon will disappear.

Figure 177: Scheduled Install

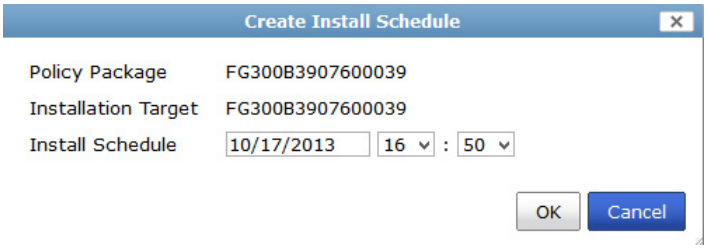


To schedule the install of a policy package to a target device:

1. Select the specific ADOM that contains the policy package you are installing from the drop-down list in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Package* heading in the pop-up menu, select *Scheduled Install*.

   The *Create Install Schedule* dialog box will be displayed.

Figure 178: Create Install Schedule



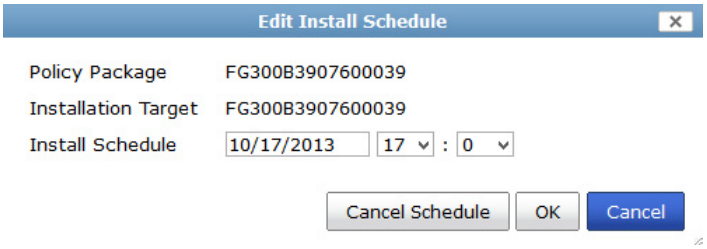
4. Configure the install schedule date and time.
5. Select OK to save the schedule. A clock icon will be displayed beside the policy package in the *Policy Package* tree.

To edit or cancel an install schedule:

1. Select the specific ADOM that contains the policy package you are installing from the drop-down list in the toolbar.
2. Click the clock icon beside the policy package in the *Policy Package* tree.

   The *Edit Install Schedul*e dialog box will be displayed.

Figure 179: Edit Install Schedule



3. Select the *Cancel Schedule* button to cancel the install schedule, and select *OK* in the confirmation dialog box. Otherwise, edit the install schedule as required and select *OK* to save the changes.

Export a policy package

To export a policy package:

1. Select the specific ADOM that contains the policy package you are exporting from the drop-down list in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Package* heading in the pop-up menu, select *Export*.

   If prompted by your web browser, select a location to where save the file, or open the file without saving.

   Policy packages are exported as CSV files.

Edit the installation targets for a policy package

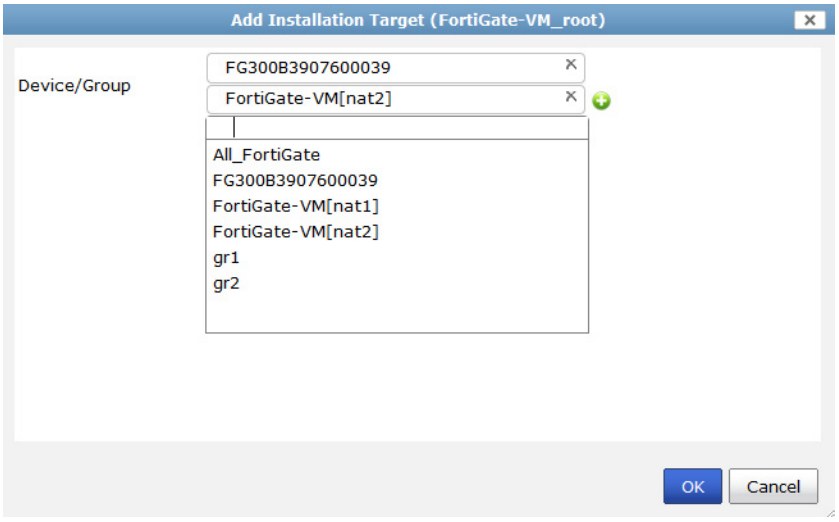
To edit a policy package's installation targets:

1. Select the specific ADOM that contains the policy package you are exporting from the drop-down list in the toolbar.
2. Select the name of the policy package from the list and select the Installation tab in the policy package toolbar.

3. Select Add in the toolbar.

   The *Add Installation Target* dialog box opens.

   Figure 180:installation target



4. Adjust the installation targets as needed, then select *OK*.

Perform a policy consistency check

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

The check will verify:

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

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

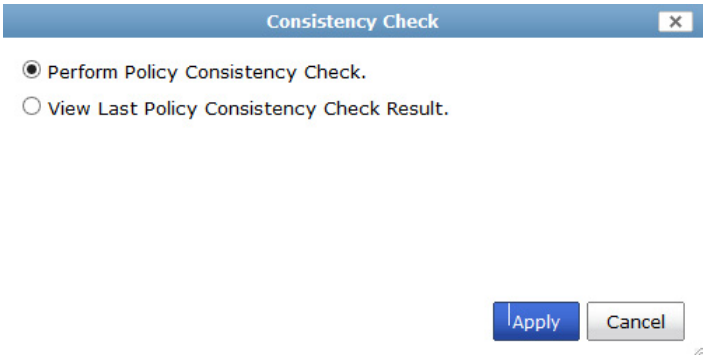
- The source and destination interface policy objects,
- The source and destination address policy objects,
- The service and schedule policy objects.

To perform a policy check:

1. Select the specific ADOM on which you would like to perform a consistency check from the drop-down list in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Package* heading in the pop-up menu, select *Policy Check*.

   The *Consistency Check* dialog box opens.

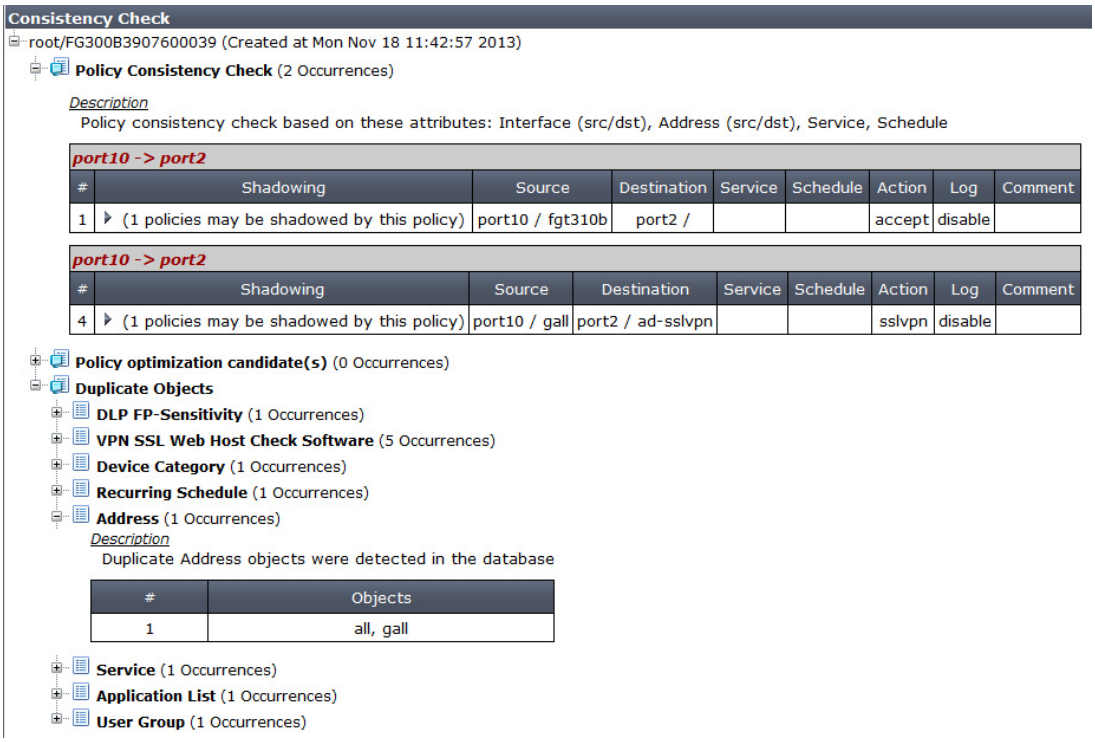
Figure 181: Consistency Check dialog box



4. To perform a new consistency check, select *Perform Policy consistency Check*, then select *Apply*.

   A policy consistency check is performed, and the results screen is shown.

Figure 182: Consistency check results window



To view the results of the last policy consistency check:

1. Select the specific ADOM on which you would like to perform a consistency check from the drop-down list in the toolbar.
2. Right-click on a policy package or folder in the *Policy Package* tree.
3. Under the *Policy Package* heading in the pop-up menu, select *Policy Check*.

   The *Consistency Check* dialog box opens.
4. To view the results of the most recent consistency check, select *View Last Policy Consistency Check Results*, then select *Apply*.

   The Consistency Check window opens, showing the results of the last policy consistency check. See Figure 182 on page 290.

Managing policies

Policies and identity policies within policy packages can be created and managed by selecting an ADOM from the drop-down list, and then selecting the policy package whose policies you are configuring. Sections can also be added to the policy list to help organize your policies.

For more information about policies, see the *FortiGate Handbook*.



Not all policy and object options are enabled by default. To configure the enabled options, go to *System Settings* > *Admin* > *Admin Settings* and select your required options. See "Administrator settings" on page 105 for more information.

Lock an ADOM

If workspace is enabled, you must lock an ADOM prior to performing any management tasks on it.

To lock an ADOM:

1. Select the specific ADOM on which you will be making changes from the drop-down list in the toolbar, or select *Global*.
2. Select the lock icon next to the drop-down list to lock the selected ADOM.

   The ADOM will now be locked, allowing you to make changes to it, and preventing other administrators from making any changes, unless lock override is enabled (see "Extend workspace to entire ADOM" on page 51).

Create a new policy or identity policy

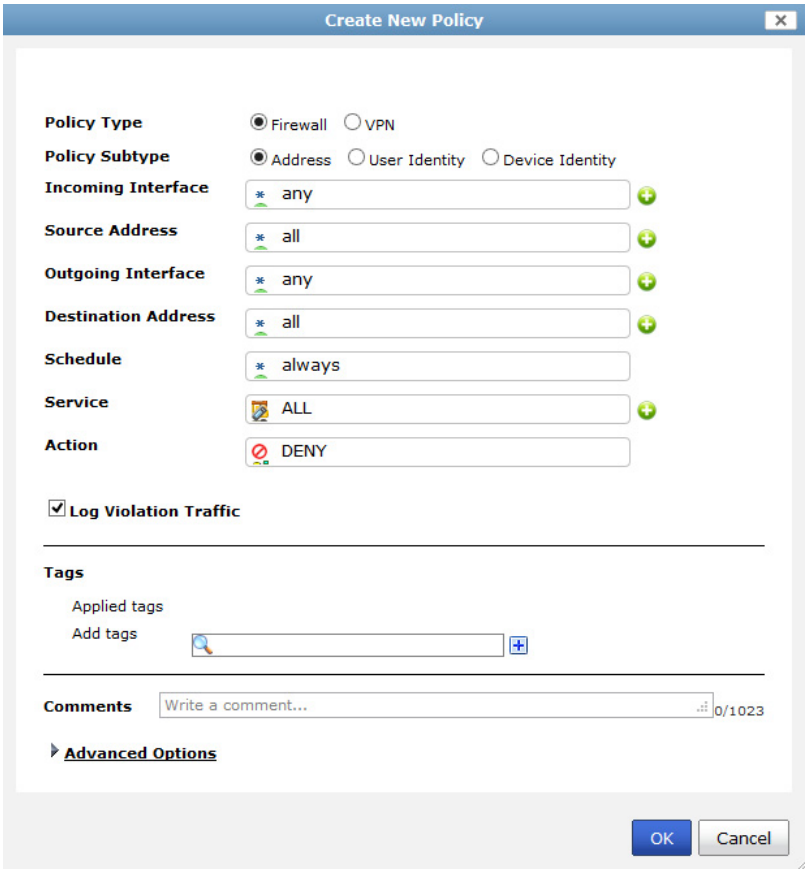
To create a new policy:

1. Select the ADOM from the drop-down list in the toolbar.
2. Select the policy package where you are creating the new policy from the tree menu.
3. Right-click on the sequence number of a current policy, or in an empty area of the content pane, and select *Create New* > *Policy* from the pop-up menu.

   If you are creating a global policy, select *Create New* > *Header Policy* or *Create New* > *Footer Policy*.

   The *Create New Policy* dialog box opens.

Figure 183: Create new policy



4. Select the type of policy you are creating in the *Policy Type* field, either *Firewall* or *VPN*.
   If you are creating a VPN policy, please skip to step 6. Otherwise continue to step 5.
5. If you are creating a firewall policy, enter the following information:

Policy Subtype	Select the firewall policy subtype. One of: *Address*, *User Identity*, *Device Identity*. The information to be added to create the policy will change according to your selection.
Incoming Interface	Select source zones from the drop-down list. Multiple zones can be selected.
Source Address	Select to add source addresses or address groups. Addresses and address groups can also be created by selecting *Create New* in the dialog box. See "Create a new object" on page 354 for more information.
Outgoing Interface	Select destination zones from the drop-down list. Multiple zones can be selected.

Destination Address	Select to add destination addresses or address groups. Addresses, address group, virtual IP, and virtual IP groups can also be created by selecting *Create New* in the dialog box. See "Create a new object" on page 354 for more information. *Note:* This option is only available if the selected subtype is *Address*.
Schedule	Select a schedule or schedules for the policy. Schedules (one time, recurring, and schedule group) can also be created by selecting *Create New* in the dialog box. See "Create a new object" on page 354 for more information. *Note:* This option is only available if the selected subtype is *Address*.
Service	Select services or service groups for the policy. Services and service groups can also be created by selecting *Create New* in the dialog box. See "Create a new object" on page 354 for more information. *Note:* This option is only available if the selected subtype is *Address*.
Action	Select an action for the policy to take, whether *ACCEPT* or *DENY*. *Note:* This option is only available if the selected subtype is *Address*.
Log Violation Traffic	Select to log violation traffic. *Note:* This option is only available if the selected subtype is *Address* and the *Action* is set to *Deny*.
NAT	Select to enable NAT. If enabled, select *Use Destination Interface Address* (with or without *Fixed Port*) or *Dynamic IP Pool* (select the pool from the list, or a new pool can be created).
Logging Options	Select one of the following: *No Log, Log Security Events,* and *Log All Sessions*. You can also select to generate logs when session starts and capture packets. *Note:* This option is only available if the selected subtype is *Address*.
Enable Web Cache	Select to enable web cache. *Note:* This option is only available if the selected subtype is *Address* or *User Identity*.
Enable WAN Optimization	Select to enable WAN optimization. If enabled, select *active* or *passive* from the drop down list, and select a profile to use for the optimization. *Note:* This option is only available if the selected subtype is *Address* or *User Identity*.
Enable Disclaimer	Select to enable the disclaimer, and enter the redirect URL.

Resolve User Name Using FSSO Agent	Select to resolve user names using the FSSO agent. *Note:* This option is only available if *Policy Subtype* is *Address* and the *Action* is *ACCEPT*.
Security Profiles	This option is only available if *Policy Subtype* is *Address* and the *Action* is *ACCEPT*.
Enable AntiVirus	Select to enable antivirus and select the profile from the drop-down list.
Enable Web Filter	Select to enable Web Filter and select the profile from the drop-down list.
Enable Application Control	Select to enable Application Control and select the profile from the drop-down list.
Enable IPS	Select to enable IPS and select the profile from the drop-down list.
Enable Email Filter	Select to enable Email Filter and select the profile from the drop-down list.
Enable DLP Sensor	Select to enable DLP Sensor and select the profile from the drop-down list.
Enable VoIP	Select to enable VoIP and select the profile from the drop-down list.
Enable ICAP	Select to enable ICAP and select the profile from the drop-down list.
Enable SSL/SSH Inspection	Select to enable SSL/SSH Inspection and select the profile from the drop-down list.
Proxy Options	Select to enable Proxy Options and select the profile from the drop-down list.
Traffic Shaping	Select to enable traffic shaping and select the traffic shaper object from the drop-down list. *Note:* This option is only available if *Policy Subtype* is *Address* and the *Action* is *ACCEPT*.
Reverse Direction Traffic Shaping	Select to enable reverse direction traffic shaping and select the traffic shaper object from the drop-down list. *Note:* This option is only available if *Policy Subtype* is *Address* and the *Action* is *ACCEPT*.
Per-IP Traffic Shaping	Select to enable per-IP traffic shaping and select the traffic shaper object from the drop-down list. *Note:* This option is only available if *Policy Subtype* is *Address* and the *Action* is *ACCEPT*.

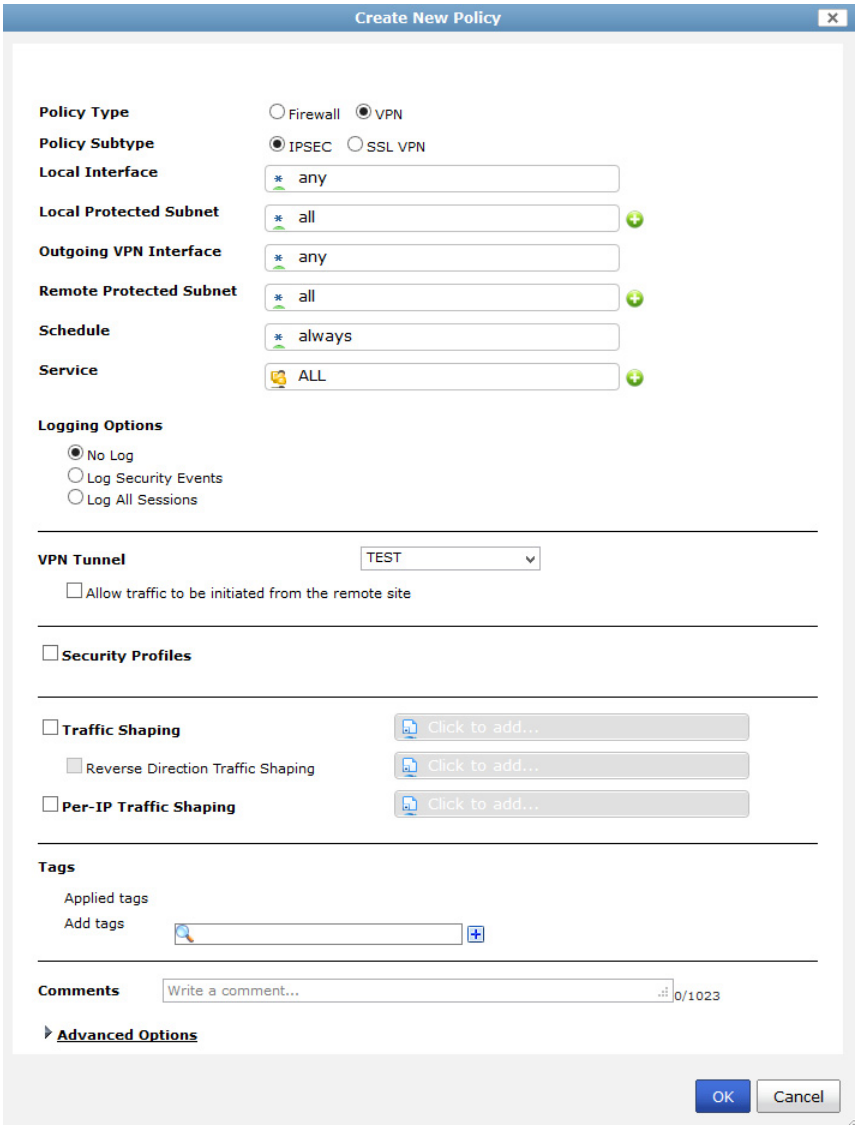
Identity Policy	Select *Add* to add an identity policy to the policy. See "To create a new identity policy:" on page 301 for more information. A certificate and customized authentication message can also be selected. *Note:* This option is only available if the selected subtype is *User Identity*.
Identity Policy	Select *Add* to add an identity policy to the policy. See "To create a new identity policy:" on page 301 for more information. A customized authentication message and device policy options can also be selected. Device policy options include: *Attempt to detect all unknown device types before implicit deny*, *Redirect all non-compliant/unregistered FortiClient compatible devices to a captive portal* (select *Windows PCs*, *Mac OSX*, *iPhone/iPad*, or *Android*), and *Prompt E-mail Collection Portal for all devices*. *Note:* This option is only available if the selected subtype is *Device Identity*.
Tags	View the tags currently applied to the policy and add new tags.
Comments	Enter a comment.
Advanced Options	For more information on advanced option, see the *FortiOS 5.0 CLI Reference*.
auth-path	Select to apply authentication-based routing. You must also specify a RADIUS server, and the RADIUS server must be configured to supply the name of an object specified in `config router auth-path`.
auth-redirect-addr	Authentication redirect address, enter the address in the text field.
auto-asic-offload	Enable or disable session offload to NP or SP processors. *Note:* This is available on models that have network processors.
custom-log-fields	Select the custom log fields from the drop-down list.
diffserv-forward	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic. If enabled, also configure `diffservcode-forward`.
diffserv-reverse	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of reverse (reply) traffic. If enabled, also configure `diffservcode-rev`.

diffservcode-forward	Enter the differentiated services code point (DSCP) value that the FortiGate unit will apply to the field of originating (forward) packets. The value is 6 bits binary. The valid range is 000000-111111. This option appears only if `diffserv-forward` is `enable`. For details and DSCP configuration examples, see the Knowledge Center article Differentiated Services Code Point (DSCP) behavior.
diffservcode-rev	Enter the differentiated services code point (DSCP) value that the FortiGate unit will apply to the field of reply (reverse) packets. The value is 6 bits binary. The valid range is 000000-111111. This option appears only if `diffserv-rev` is `enable` For details and DSCP configuration examples, see the Knowledge Center article Differentiated Services Code Point (DSCP) behavior.
fall-through-unauthenticated	Enable to allow an unauthenticated user to skip authentication rules and possibly match another policy.
fsso-agent-for-ntlm	Select the FSSO agent for NTLM from the drop-down list.
log-unmatched-traffic	Enable or disabling logging dropped traffic for policies with `identity-based` enabled.
match-vip	If you want to explicitly drop a packet that is not matched with a firewall policy and write a log message when this happens, you can add a general policy (source and destination address set to ANY) to the bottom of a policy list and configure the firewall policy to DENY packets and record a log message when a packet is dropped. In some cases, when a virtual IP performs destination NAT (DNAT) on a packet, the translated packet may not be accepted by a firewall policy. If this happens, the packet is silently dropped and therefore not matched with the general policy at the bottom of the policy list. To catch these packets, enable `match-vip` in the general policy. Then the DNATed packets that are not matched by a VIP policy are matched with the general policy where they can be explicitly dropped and logged.
natip	Enter the NAT IP address in the text field.
ntlm-enabled-browsers	Enter a value in the text field.
ntlm-guest	Select to enable or disable NTLM guest.
permit-any-host	Enable to accept UDP packets from any host. This can help support the FaceTime application on NAT'd iPhones.
permit-stun-host	Enable to accept UDP packets from any STUN host. This can help support the FaceTime application on NAT'd iPhones.

profile-type	Select the profile type from the drop-down list.
rtp-addr	Select the RTP address from the drop-down list. *Note:* This field is only available when `rtp-nat` is enabled.
rtp-nat	Enable to apply source NAT to RTP packets received by the firewall policy. This field is used for redundant SIP configurations. If `rtp-nat` is enabled you must add one or more firewall addresses to the `rtp-addr` field.
schedule-timeout	Enable to force session to end when policy schedule end time is reached.
send-deny-packet	Enable to send a packet in reply to denied TCP, UDP or ICMP traffic. When `deny-tcp-with-icmp` is enabled in system settings, a Communication Prohibited ICMP packet is sent. Otherwise, denied TCP traffic is sent a TCP reset.
session-ttl	Enter a value for the session time-to-live (TTL). Enter a value between 300 to 604800 or enter 0 for no limitation.
tcp-mss-receiver	Enter a value for the receiver's TCP MSS.
tcp-mss-sender	Enter a value for the sender's TCP MSS.
timeout-send-rst	Enable sending a TCP reset when an application session times out.
transaction-based	Select to enable or disable this feature.
wccp	Select to enable or disable Web Cache Communication Protocol (WCCP).
web-auth-cookie	Enable to reduce the number of authentication requests to the authentication server when session-based authentication is applied using explicit web proxy. This is only available when session based authentication is enabled.

6. If you are creating a VPN policy, select *VPN* in the *Policy Type* field.

Figure 184: Create new policy (VPN)



The *Create New Policy* dialog box content changes to the VPN options. Enter the following information:

Policy Subtype	Select the VPN policy subtype, either *IPSEC* or *SSL VPN*. The information to be added to create the policy will change according to your selection.
Incoming Interface	Select source zones from the drop-down list. Multiple zones can be selected. *Note:* This option is only available if the selected subtype is *SSL VPN*.
Remote Address	Select to add remote addresses or address groups. Addresses and address groups can also be created by selecting *Create New* in the dialog box. See "Create a new object" on page 354 for more information. *Note:* This option is only available if the selected subtype is *SSL VPN*.

Local Interface	Select source zones from the drop-down list. Multiple zones can be selected.
Local Protected Subnet	Select to add addresses or address groups. Addresses and address groups can also be created by selecting *Create New* in the dialog box. See "Create a new object" on page 354 for more information.
Outgoing VPN Interface	Select destination zones from the drop-down list. Multiple zones can be selected. *Note:* This option is only available if the selected subtype is *IPSEC*.
Remote Protected Subnet	Select to add addresses or address groups. Addresses and address groups can also be created by selecting *Create New* in the dialog box. See "Create a new object" on page 354 for more information. *Note:* This option is only available if the selected subtype is *IPSEC*.
Schedule	Select a schedule or schedules for the policy. Schedules can also be created by selecting *Create New* in the dialog box. See "Create a new object" on page 354 for more information. *Note:* This option is only available if the selected subtype is *IPSEC*.
Service	Select services or service groups for the policy. Services and service groups can also be created by selecting *Create New* in the dialog box. See "Create a new object" on page 354 for more information. *Note:* This option is only available if the selected subtype is *IPSEC*.
Logging Options	Select the policy logging options: *No Log*, *Log Security Events*, or *Log All Sessions*. If the last option is selected, *Generate Logs when Session Starts* and *Capture Packets* can also be selected. *Note:* This option is only available if the selected subtype is *IPSEC*.
SSL VPN Users	Select *Add* to add SSL VPN users to the policy. *Note:* This option is only available if the selected subtype is *SSL VPN*.
SSL Client Certificate Restrictive	Select to make the SSL client certificate restrictive. If enabled, select the cipher strength: *Any*, *High >= 164*, or *Medium >= 128*. *Note:* This option is only available if the selected subtype is *SSL VPN*.
VPN Tunnel	Select a VPN tunnel from the drop-down list. *Allow traffic to be initiated from the remote site* can also be enabled. *Note:* This option is only available if the selected subtype is *IPSEC*.
Security Profiles	Enable security profiles, then select the specific profiles and their respective profile object. Profiles include: *Antivirus, Web Filter, Application Control, IPS, Email Filter, DLP Sensor, VoIP, ICAP, SSL/SSH Inspection,* and *Proxy Options*. *Note:* This option is only available if the selected subtype is *IPSEC*. For more information see "Security Profiles" on page 294.

Traffic Shaping	Select to enable traffic shaping, then select a shaping option from the drop down list. If enabled, you can also select *Reverse Direction Traffic Shaping* and a shaping option from the drop down list. *Note:* This option is only available if the selected subtype is *IPSEC*.
Per-IP Traffic Shaping	Select to enable per-IP traffic shaping, then select a shaping option from the drop down list. *Note:* This option is only available if the selected subtype is *IPSEC*.
Tags	View the tags currently applied to the policy and add new tags.
Comments	Enter a comment.
Advanced Options	Select advanced policy related options. For a list of these options, see "Advanced Options" on page 295.

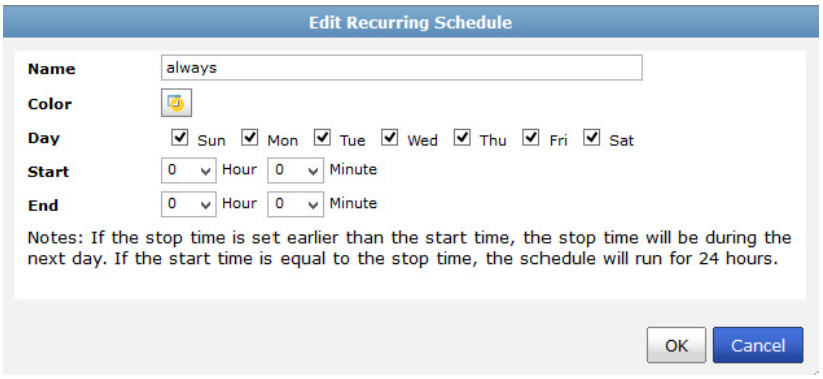
7. Select *OK* to create the policy. You can select to enable or disable the policy in the right-click menu.

Edit the policy schedule:

1. Select *Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Schedule* column and select *Edit* in the menu.

   The *Edit Recurring Schedule* dialog box is displayed.

Figure 185: Edit Recurring Schedule



3. Configure the following settings:

Name	Edit the schedule name as required.
Color	Select the icon to select an custom icon to display next to the schedule name.
Day	Select the days of the week for the custom schedule.
Start	Select the schedule start time.
End	Select the schedule end time.

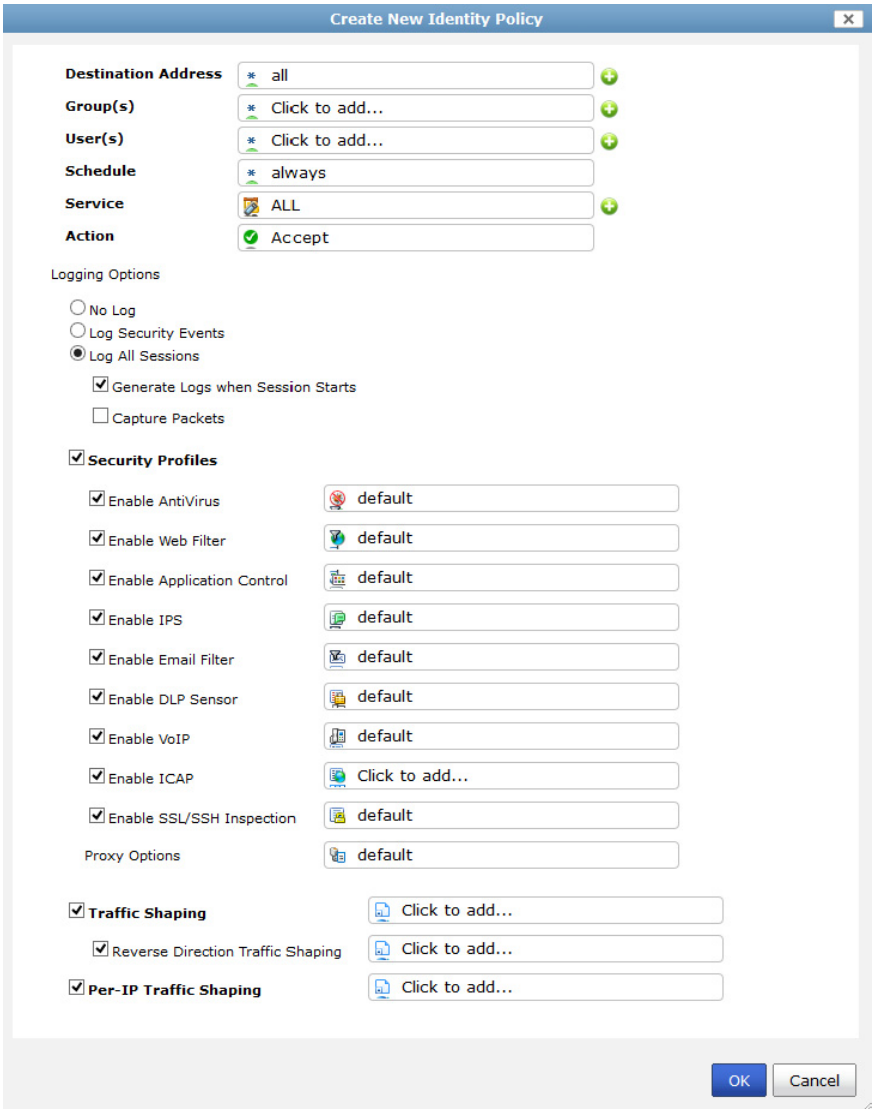
4. Select *OK* to save the schedule. The custom schedule will be added to *Objects* > *Firewall Objects* > *Schedule*.

To create a new identity policy:

1. Select the ADOM from the drop-down list in the toolbar.
2. Select the policy package where you are creating the new identity policy from the tree menu.
3. Right-click on the sequence number of a current policy, or in an empty area of the content pane and select *Create New* > *Identity Policy* from the pop-up menu.

   The *Create New Identity Policy* dialog box opens.

Figure 186: Create new identity policy



4. Enter the following information:

Destination Address	Select to add destination addresses or address groups. Addresses and address groups can also be created by selecting *Create New* in the dialog box. See "Create a new object" on page 354 for more information.
Group(s)	Select to add a group or groups to the policy.

User(s)	Select to add a user or users to the policy.
Schedule	Select a schedule or schedules for the policy. Schedules can also be created by selecting *Create New* in the dialog box. See "Create a new object" on page 354 for more information.
Service	Select services or service groups for the policy. Services and service groups can also be created by selecting *Create New* in the dialog box. See "Create a new object" on page 354 for more information.
Action	Select an action for the policy to take, whether *ACCEPT* or *DENY*.
Logging Options	Select the policy logging options: *No Log*, *Log Security Events*, or *Log All Sessions*. If the last option is selected, *Generate Logs when Session Starts* and *Capture Packets* can also be selected.
Security Profiles	Enable security profiles, then select the specific profiles and their respective profile object. Profiles include: *Antivirus, Web Filter, Application Control, IPS, Email Filter, DLP Sensor, VoIP, ICAP, SSL/SSH Inspection,* and *Proxy Options*. For more information see "Security Profiles" on page 294.
Traffic Shaping	Select to enable traffic shaping, then select a shaping option from the drop down list. If enabled, you can also select *Reverse Direction Traffic Shaping* and a shaping option from the drop down list.
Per-IP Traffic Shaping	Select to enable per-IP traffic shaping, then select a shaping option from the drop down list.

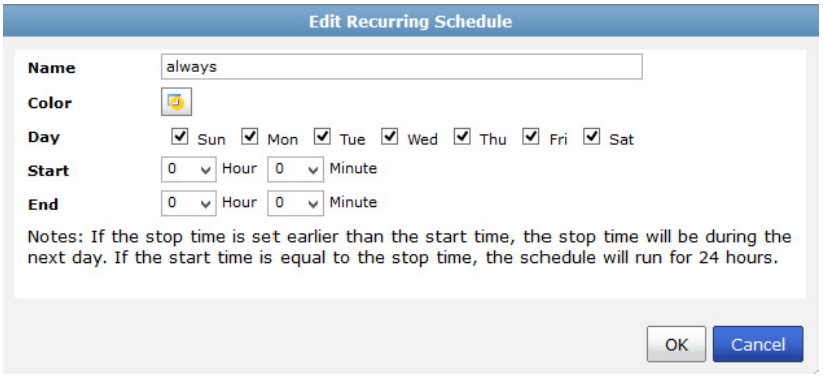
5. Select *OK* to create the identity policy. You can select to enable or disable the policy in the right-click menu.

Edit the policy schedule:

1. Select *Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Schedule* column and select *Edit* in the menu.

   The *Edit Recurring Schedule* dialog box is displayed.

Figure 187: Edit Recurring Schedule



3. Configure the following settings:

Name	Edit the schedule name as required.
Color	Select the icon to select an custom icon to display next to the schedule name.
Day	Select the days of the week for the custom schedule.
Start	Select the schedule start time.
End	Select the schedule end time.

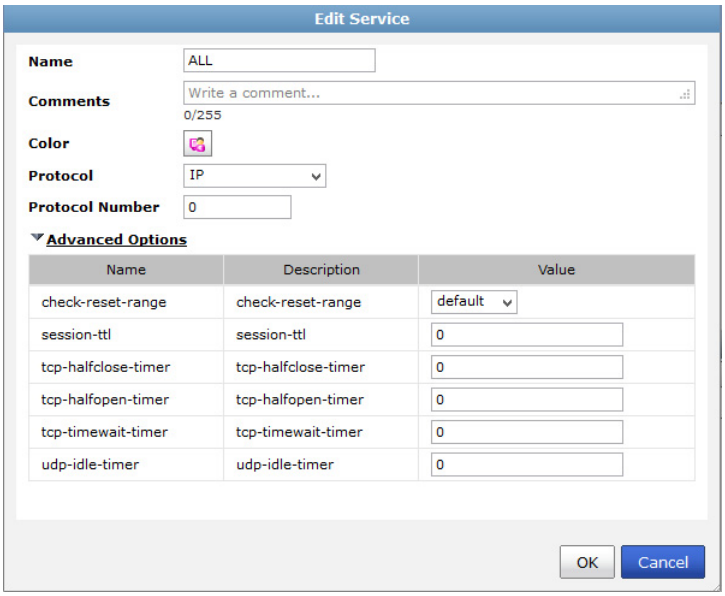
4. Select *OK* to save the schedule. The custom schedule will be added to *Objects* > *Firewall Objects* > *Schedule*.

Edit the policy service:

1. Select *Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Service* column and select *Edit* in the menu.

   The *Edit Service* dialog box is displayed.

Figure 188: Edit Service



3. Configure the following settings:

Name	Edit the service name as required.
Comments	Enter an optional comment.
Color	Select the icon to select an custom icon to display next to the service name.
Protocol	Select the protocol from the drop-down list. Select one of the following: *TCP/UDP/SCTP, ICMP, ICMP6,* or *IP*.

IP/FQDN	Enter the IP or FQDN. *Note:* This menu item is available when *Protocol* is set to *TCP/UDP/SCTP*. You can then define the protocol, source port and destination port in the table.
Type	Enter the type in the text field. *Note:* This menu item is available when *Protocol* is set to *ICMP* and *ICMP6*.
Code	Enter the code in the text field. *Note:* This menu item is available when *Protocol* is set to *ICMP* and *ICMP6*.
Protocol Number	Enter the protocol number in the text field. *Note:* This menu item is available when *Protocol* is set to *IP.*
Advanced Options	For more information on advanced option, see the *FortiOS 5.0 CLI Reference*.
check-reset-range	Configure ICMP error message verification. • `disable` — The FortiGate unit does not validate ICMP error messages. • `strict` — If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) | TCP(C,D) header, then if FortiOS can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If is enabled the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the `anti-replay` option checks packets. • `default` — Use the global setting defined in `system global`. *Note:* This field is available when `protocol` is `TCP/UDP/SCTP`. *Note:* This field is not available if `explicit-proxy` is enabled.
session-ttl	Enter the default session timeout in seconds. The valid range is from 300 - 604 800 seconds. Enter `0` to use either the per-policy session-ttl or per-VDOM session-ttl, as applicable. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`.
tcp-halfclose-timer	Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is from 1 to 86400 seconds. Enter `0` to use the global setting defined in `system global`. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`.

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

4. Select *OK* to save the service. The custom service will be added to *Objects* > *Firewall Objects* > *Service*.

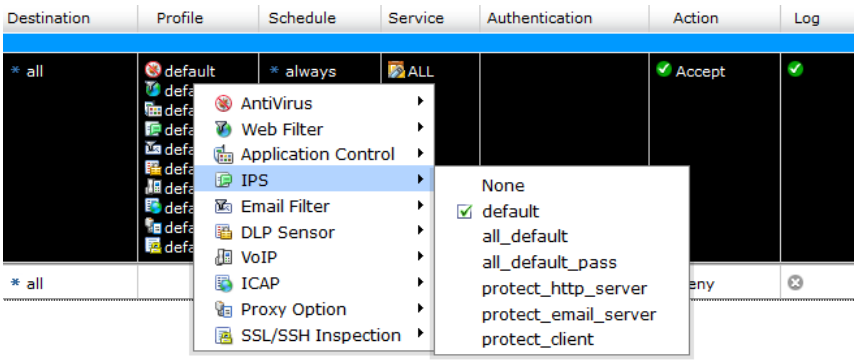
To edit the policy action:

1. Select *Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Action* column.
3. Select either *Accept* or *Deny* in the menu.

To edit the policy security profiles:

1. Select *Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Profile* column.

Figure 189: Profile right-click menu



3. When you select each security profile option in the right-click menu, you can select the profile object.

To edit policy logging:

1. Select *Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Log* column.
3. You can select to disable logging, log all security events, or log all session in the menu.

Interface Policy

The Interface Policy tab allows you to create, edit, delete, and clone interface policies. The following information is displayed for these policies: Seq.#, Interface (source interface), Source (source address), Destination (destination address), Service, IPS Sensor (profile), Application Sensor (profile), AntiVirus (profile), Web Filter (profile), DLP Sensor (profile), Email Filter (profile), and Install On (installation targets).



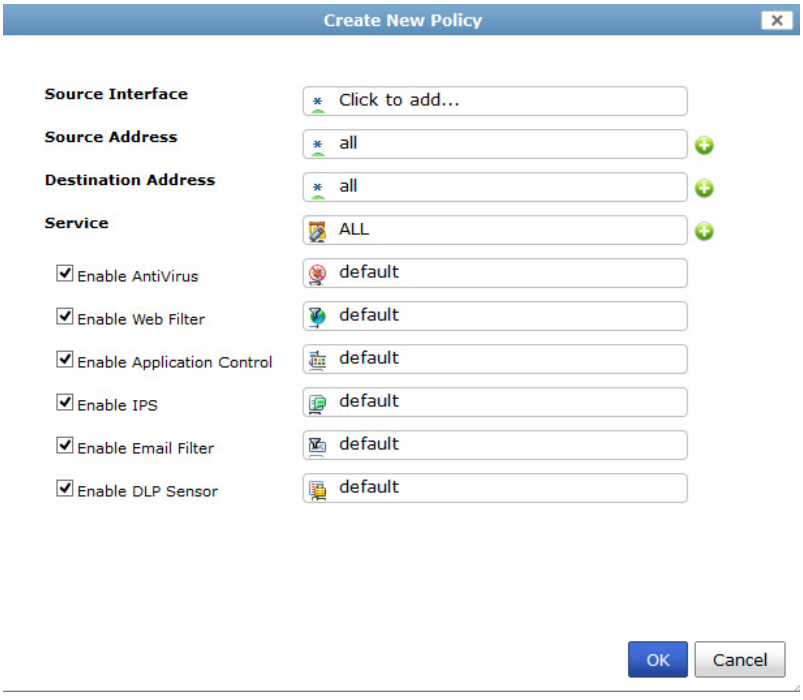
Select *Display Options* in the *Policy & Objects* tab, and toggle the *Interface Policy* switch to display this option in the Policy Package tab bar.

To create a new interface policy:

1. Select the ADOM from the drop-down list in the toolbar.
2. Select the policy package where you are creating the new identity policy from the tree menu.
3. Select *Interface Policy* in the policy toolbar.
4. Right-click on the sequence number of a current policy, or in an empty area of the content pane and select *Create New* from the pop-up menu.

   The *Create New Policy* dialog box opens.

Figure 190: Interface Policy



5. Configure the following settings:

Source Interface	Select the source zone from the drop-down list.
Source Address	Select the source address from the drop-down list. You can create a new address or address group in the *Add Source Address* window.
Destination Address	Select the destination address from the drop-down list. You can create a new address or address group in the *Add Destination Address* dialog box.
Service	Select the service from the drop-down list. You can create a new service or service group in the *Add Service* dialog box.
Enable AntiVirus	Select to enable antivirus and select the profile from the drop-down list.
Enable Web Filter	Select to enable Web Filter and select the profile from the drop-down list.
Enable Application Control	Select to enable Application Control and select the profile from the drop-down list.
Enable IPS	Select to enable IPS and select the profile from the drop-down list.
Enable Email Filter	Select to enable Email Filter and select the profile from the drop-down list.
Enable DLP Sensor	Select to enable DLP Sensor and select the profile from the drop-down list.

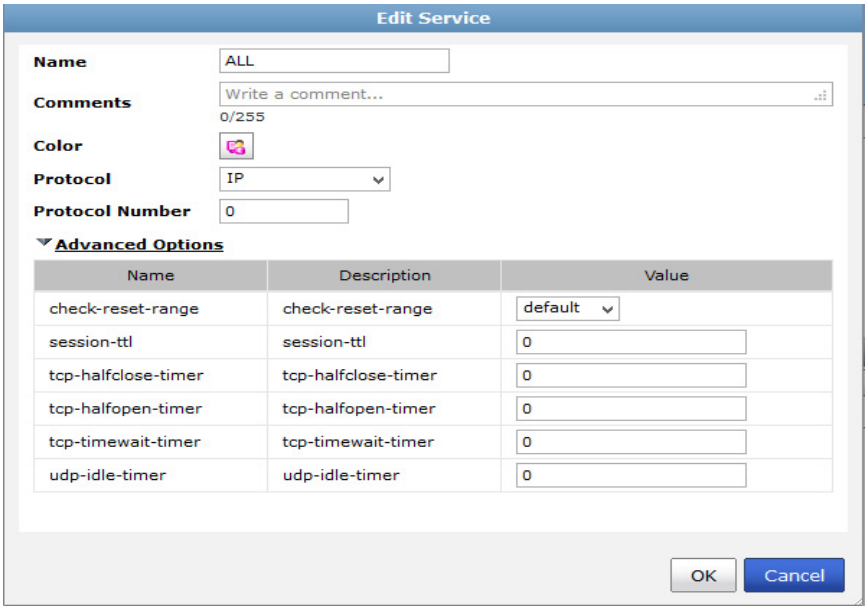
6. Select *OK* to save the setting. You can select to enable or disable the policy in the right-click menu.

Edit the policy service:

1. Select *Interface Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Service* column and select *Edit* in the menu.

   The *Edit Service* dialog box is displayed.

Figure 191: Edit Service



3. Configure the following settings:

Name	Edit the service name as required.
Comments	Enter an optional comment.
Color	Select the icon to select an custom icon to display next to the service name.
Protocol	Select the protocol from the drop-down list. Select one of the following: *TCP/UDP/SCTP, ICMP, ICMP6,* or *IP*.
IP/FQDN	Enter the IP or FQDN. *Note:* This menu item is available when *Protocol* is set to *TCP/UDP/SCTP*. You can then define the protocol, source port and destination port in the table.
Type	Enter the type in the text field. *Note:* This menu item is available when *Protocol* is set to *ICMP* and *ICMP6*.
Code	Enter the code in the text field. *Note:* This menu item is available when *Protocol* is set to *ICMP* and *ICMP6*.
Protocol Number	Enter the protocol number in the text field. *Note:* This menu item is available when *Protocol* is set to *IP.*
Advanced Options	For more information on advanced option, see the *FortiOS 5.0 CLI Reference*.

check-reset-range	Configure ICMP error message verification. • `disable` — The FortiGate unit does not validate ICMP error messages. • `strict` — If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) | TCP(C,D) header, then if FortiOS can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If is enabled the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the `anti-replay` option checks packets. • `default` — Use the global setting defined in `system global`. *Note:* This field is available when `protocol` is `TCP/UDP/SCTP`. *Note:* This field is not available if `explicit-proxy` is enabled.
session-ttl	Enter the default session timeout in seconds. The valid range is from 300 - 604 800 seconds. Enter `0` to use either the per-policy session-ttl or per-VDOM session-ttl, as applicable. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`
tcp-halfclose-timer	Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is from 1 to 86400 seconds. Enter `0` to use the global setting defined in `system global`. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`.
tcp-halfopen-timer	Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded. The valid range is from 1 to 86400 seconds. Enter `0` to use the global setting defined in `system global`. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`.

tcp-timewait-timer	Set the length of the TCP TIME-WAIT state in seconds. As described in RFC 793, the “TIME-WAIT state represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request”. Reducing the time of the TIME-WAIT state means the FortiGate unit can close terminated sessions faster which means more new sessions can be opened before the session limit is reached. The valid range is 0 to 300 seconds. A value of 0 sets the TCP TIME-WAIT to 0 seconds. Enter `0` to use the global setting defined in `system global`. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`.
udp-idle-timer	Enter the number of seconds before an idle UDP connection times out. The valid range is from 1 to 86400 seconds. Enter `0` to use the global setting defined in `system global`. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`.

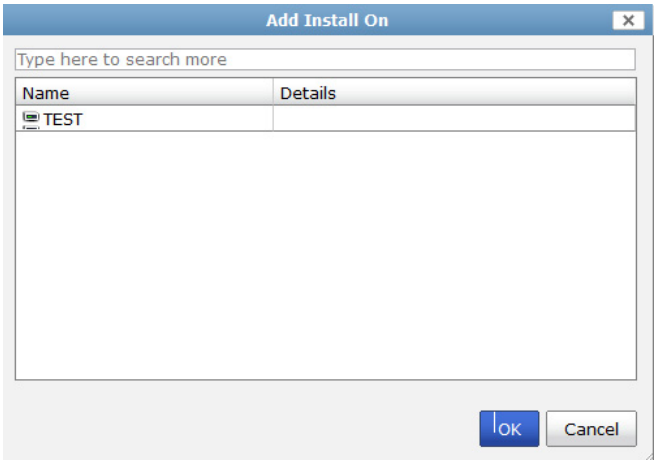
4. Select *OK* to save the service. The custom service will be added to *Objects* > *Firewall Objects* > *Service*.

To edit the installation target:

1. Select *Interface Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Install On* column and select *Add Object(s)* in the menu.

   The *Add Install On* dialog box is displayed.

Figure 192: Add Install On



3. Select the installation targets from the list and select *OK*. To edit the installation targets, select the *Installation* tab in the Policy Package tab bar and select *Edit Targets* in the toolbar.

Central NAT table

The central NAT table enables you to define, and control with more granularity, the address translation performed by the FortiGate unit. With the NAT table, you can define the rules which dictate the source address or address group and which IP pool the destination address uses.

While similar in functionality to IP pools, where a single address is translated to an alternate address from a range of IP addresses, with IP pools there is no control over the translated port. When using the IP pool for source NAT, you can define a fixed port to guarantee the source port number is unchanged. If no fix port is defined, the port translation is randomly chosen by the FortiGate unit. With the central NAT table, you have full control over both the IP address and port translation.

The FortiGate unit reads the NAT rules in a top-down methodology, until it hits a matching rule for the incoming address. This enables you to create multiple NAT policies that dictate which IP pool is used based on the source address. The NAT policies can be rearranged within the policy list as well. NAT policies are applied to network traffic after a security policy.

The Central NAT tab allows you to create, edit, delete, and clone central NAT entries. The following information is displayed for these entries: NAT ID, Status, Original Address, Original Source Port, Translated Address, Translated Port, and Last Modified (admin and date and time that the entry was last modified). Select the checkbox in the Status column to enable or disable the central NAT entry.



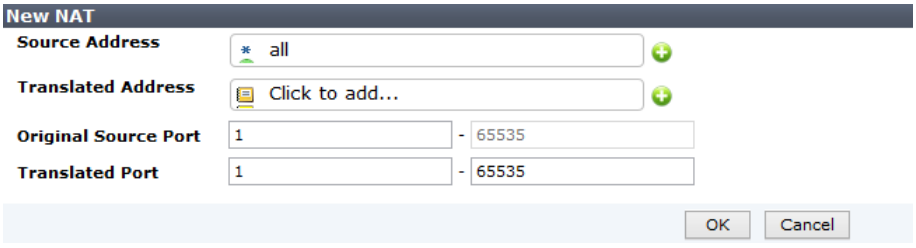
Select *Display Options* in the *Policy & Objects* tab, and toggle the *Central NAT* switch to display this option in the Policy Package tab bar.

To create a new central NAT entry:

1. Select the ADOM from the drop-down list in the toolbar.
2. Select the policy package where you are creating the new interface policy from the tree menu.
3. Select *Central NAT* in the policy toolbar.
4. Select *Create New* from the toolbar.

   The *New NAT* page opens.

Figure 193: Central NAT



5. Configure the following settings:

Source Address	Select the source address from the drop-down list. You can select to create a new address or address group in the *Source Address* dialog box.
Translated Address	Select the translated address from the drop-down list. You can select to create a new IP Pool in the *Translated Address* dialog box.

Original Source Port	Enter the original source port range.
Translated Port	Enter the translated port range.

6. Select *OK* to save the setting.

IPv6 Policy

IPv6 security policies are created both for an IPv6 network, and a transitional network. A transitional network is a network that is transitioning over to IPv6, but must still have access to the Internet or must connect over an IPv4 network.

These policies allow for this specific type of traffic to travel between the IPv6 and IPv4 networks. The IPv6 options for creating these policies is hidden by default.

To create a new IPv6 Policy, go to the *Policy & Objects* tab and select *IPv6 Policy* in the policy toolbar. Right-click the content pane and select *Create New* > *Policy* or *Create New* > *Identity Policy*. See "Create a new policy or identity policy" on page 291 for more information.



Select *Display Options* in the *Policy & Objects* tab, and toggle the *IPv6 Policy* switch to display this option in the Policy Package tab bar.

IPv6 Interface Policy

To create a new IPv6 Interface Policy, go to the *Policy & Objects* tab and select *IPv6 Interface Policy* in the policy toolbar. Right-click the content pane and select *Create New*. See "Interface Policy" on page 306 for more information.



Select *Display Options* in the *Policy & Objects* tab, and toggle the *IPv6 Interface Policy* switch to display this option in the Policy Package tab bar.

DoS Policy

The DoS Policy tab allows you to create, edit, delete, and clone DoS policies. The following information is displayed for these policies: Seq.# (sequence number), Interface (incoming interface), Source (source address), Destination (destination address), Service, and Install On (installation targets).



Select *Display Options* in the *Policy & Objects* tab, and toggle the *DoS Policy* switch to display this option in the Policy Package tab bar.

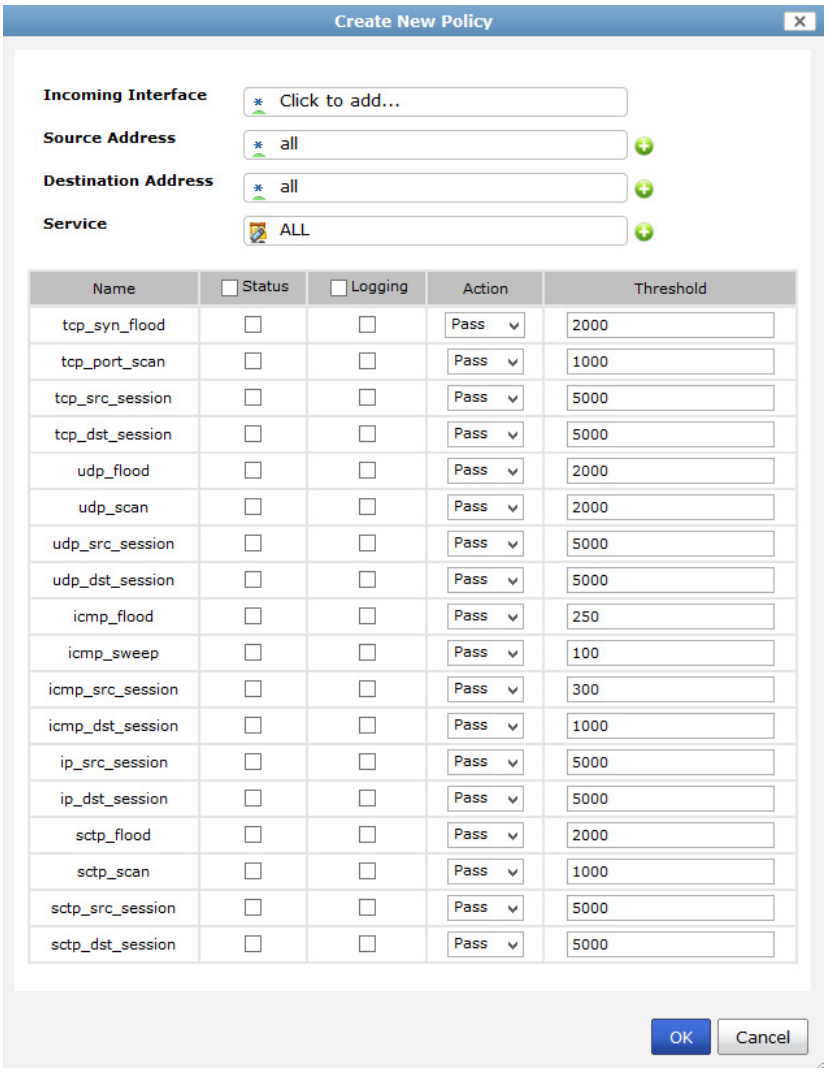
To create a DoS policy:

1. Select the ADOM from the drop-down list in the toolbar.
2. Select the policy package where you are creating the new DoS policy from the tree menu.
3. Select *DoS Policy NAT* in the policy toolbar.

4. Right-click on the sequence number of a current policy, or in an empty area of the content pane and select *Create New* from the pop-up menu.

   The *Create New Policy* dialog box opens.

Figure 194: New DoS Policy



5. Configure the following settings:

Incoming Interface	Select the incoming interface from the drop-down list.
Source Address	Select the source address from the drop-down list. You can select to create a new address or address group in the *Source Address* dialog box.
Destination Address	Select the destination address from the drop-down list. You can create a new address or address group in the *Add Destination Address* dialog box.
Service	Select the service from the drop-down list. You can create a new service or service group in the *Add Service* dialog box.
tcp_syn_flood	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.

tcp_port_scan	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
tcp_src_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
tcp_dst_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
udp_flood	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
udp_scan	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
udp_src_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
udp_dst_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
icmp_flood	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
icmp_sweep	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
icmp_src_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
icmp_dst_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
ip_src_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
ip_dst_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
scttp_flood	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
sctp_scan	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
sctp_src_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
sctp_dst_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.

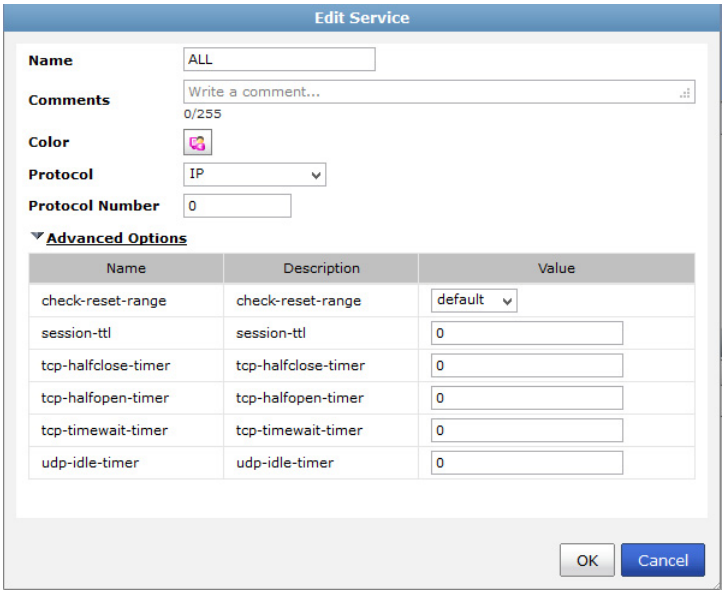
6. Select *OK* to save the setting.

Edit the policy service:

1. Select *DoS Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Service* column and select *Edit* in the menu.

   The *Edit Service* dialog box is displayed.

Figure 195: Edit Service



3. Configure the following settings:

Name	Edit the service name as required.
Comments	Enter an optional comment.
Color	Select the icon to select an custom icon to display next to the service name.
Protocol	Select the protocol from the drop-down list. Select one of the following: *TCP/UDP/SCTP, ICMP, ICMP6,* or *IP*.
IP/FQDN	Enter the IP or FQDN. *Note:* This menu item is available when *Protocol* is set to *TCP/UDP/SCTP*. You can then define the protocol, source port and destination port in the table.
Type	Enter the type in the text field. *Note:* This menu item is available when *Protocol* is set to *ICMP* and *ICMP6*.
Code	Enter the code in the text field. *Note:* This menu item is available when *Protocol* is set to *ICMP* and *ICMP6*.
Protocol Number	Enter the protocol number in the text field. *Note:* This menu item is available when *Protocol* is set to *IP.*
Advanced Options	For more information on advanced option, see the *FortiOS 5.0 CLI Reference*.

check-reset-range	Configure ICMP error message verification. • `disable` — The FortiGate unit does not validate ICMP error messages. • `strict` — If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) | TCP(C,D) header, then if FortiOS can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If is enabled the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the `anti-replay` option checks packets. • `default` — Use the global setting defined in `system global`. *Note:* This field is available when `protocol` is `TCP/UDP/SCTP`. *Note:* This field is not available if `explicit-proxy` is enabled.
session-ttl	Enter the default session timeout in seconds. The valid range is from 300 - 604 800 seconds. Enter `0` to use either the per-policy session-ttl or per-VDOM session-ttl, as applicable. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`
tcp-halfclose-timer	Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is from 1 to 86400 seconds. Enter `0` to use the global setting defined in `system global`. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`.
tcp-halfopen-timer	Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded. The valid range is from 1 to 86400 seconds. Enter `0` to use the global setting defined in `system global`. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`.

tcp-timewait-timer	Set the length of the TCP TIME-WAIT state in seconds. As described in RFC 793, the “TIME-WAIT state represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request”. Reducing the time of the TIME-WAIT state means the FortiGate unit can close terminated sessions faster which means more new sessions can be opened before the session limit is reached. The valid range is 0 to 300 seconds. A value of 0 sets the TCP TIME-WAIT to 0 seconds. Enter `0` to use the global setting defined in `system global`. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`.
udp-idle-timer	Enter the number of seconds before an idle UDP connection times out. The valid range is from 1 to 86400 seconds. Enter `0` to use the global setting defined in `system global`. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`.

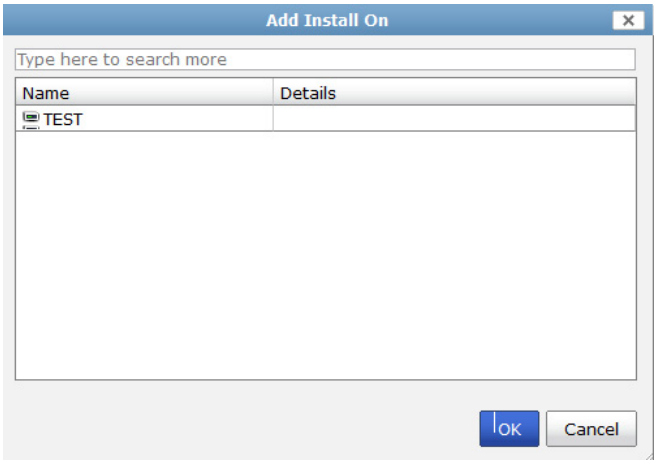
4. Select *OK* to save the service. The custom service will be added to *Objects* > *Firewall Objects* > *Service*.

To edit the installation target:

1. Select *NAT64 Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Install On* column and select *Add Object(s)* in the menu.

   The *Add Install On* dialog box is displayed.

Figure 196: Add Install On



3. Select the installation targets from the list and select *OK*. To edit the installation targets, select the *Installation* tab in the Policy Package tab bar and select *Edit Targets* in the toolbar.

IPv6 DoS Policy

The IPv6 DoS Policy tab allows you to create, edit, delete, and clone IPv6 DoS policies. For more information on configuring DoS policies, see “DoS Policy” on page 312.



Select *Display Options* in the *Policy & Objects* tab, and toggle the *IPv6 DoS Policy* switch to display this option in the Policy Package tab bar.

NAT46 Policy

Use NAT46 policies for IPv6 environments where you want to expose certain services to the public IPv4 Internet. You will need to configure a virtual IP to permit the access. The NAT46 Policy tab allows you to create, edit, delete, and clone NAT46 policies.



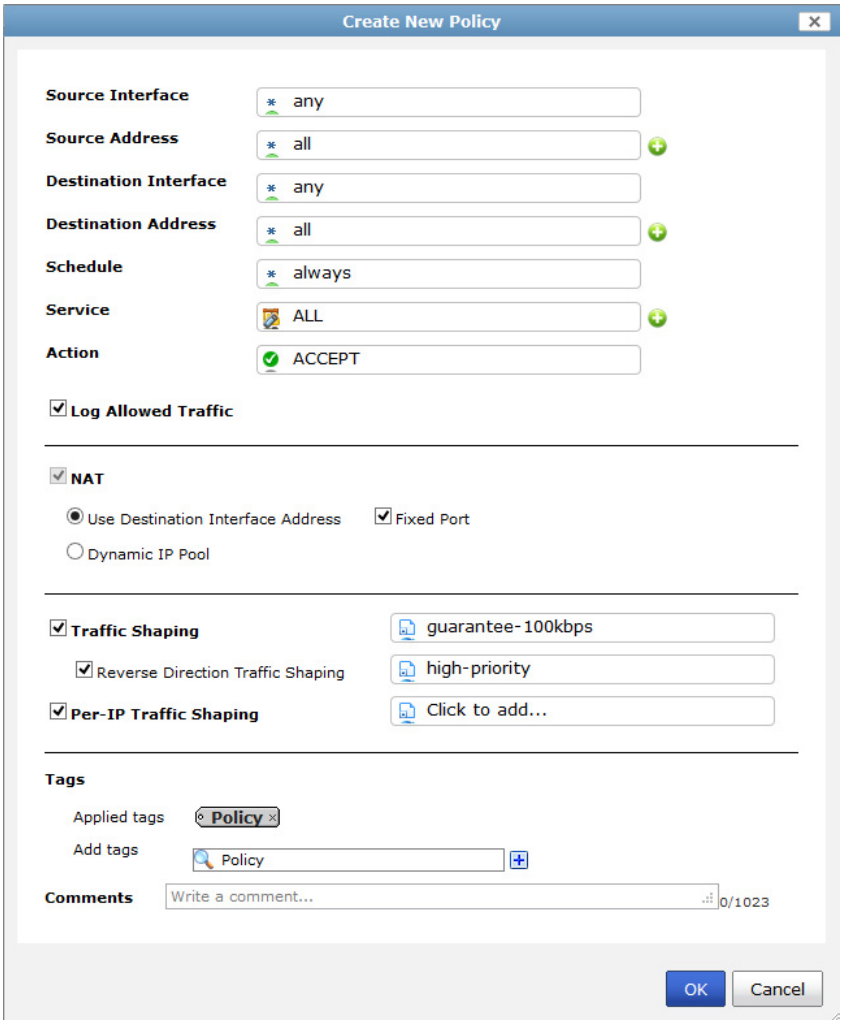
Select *Display Options* in the *Policy & Objects* tab, and toggle the *NAT46 Policy* switch to display this option in the Policy Package tab bar.

To create a NAT46 policy:

1. Select the ADOM from the drop-down list in the toolbar.
2. Select the policy package where you are creating the new NAT46 policy from the tree menu.
3. Select *NAT46 Policy* in the policy toolbar.
4. Right-click on the sequence number of a current policy, or in an empty area of the content pane and select *Create New* from the pop-up menu.

   The *Create New Policy* dialog box opens.

Figure 197:NAT46 Policy



5. Configure the following settings:

Source Interface	Select the source interface from the drop-down list.
Source Address	Select the source address from the drop-down list. You can select to create a new address or address group in the *Source Address* dialog box.
Destination Interface	Select the destination interface from the drop-down list.
Destination Address	Select the destination address from the drop-down list. You can create a new address or address group in the *Add Destination Address* dialog box.
Schedule	Select a schedule or schedules for the policy. Schedules can also be created by selecting *Create New* in the dialog box. See "Create a new object" on page 354 for more information.
Service	Select the service from the drop-down list. You can create a new service or service group in the *Add Service* dialog box.

Action	Select an action for the policy to take, whether *ACCEPT* or *DENY*. When *Action* is set to *Accept*, you can configure *NAT* and *Traffic Shaping*.
Log Allowed Traffic **Log Violation Traffic**	Select to log allowed traffic/violation traffic. *Note:* This setting is dependent on the *Action* setting.
NAT	NAT is enabled by default for this policy type.
Use Destination Interface Access	Select to use the destination interface address.
Fixed Port	Select to enable fixed port.
Dynamic IP Pool	Select to enable dynamic IP pool and select the dynamic IP pool from the drop-down list.
Traffic Shaping	Select to enable traffic shaping and select a default or custom traffic shaper object from the drop-down list.
Reverse Direction Traffic Shaping	Select to enable reverse direction traffic shaping and select a default or custom traffic shaper object from the drop-down list.
Per-IP Traffic Shaping	Select to enable per-IP traffic shaping and select the related object from the drop-down list.
Tags	You can add tags for tag management. Enter a tag in the text field and select the plus (+) icon to apply the tag to the policy.
Comments	Enter optional comments for the policy.

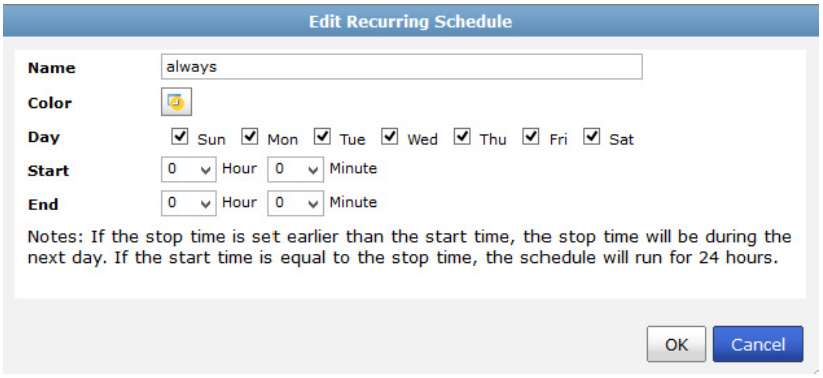
6. Select *OK* to save the policy.

Edit the policy schedule:

1. Select *NAT46 Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Schedule* column and select *Edit* in the menu.

   The *Edit Recurring Schedule* dialog box is displayed.

Figure 198: Edit Recurring Schedule



3. Configure the following settings:

Name	Edit the schedule name as required.
Color	Select the icon to select an custom icon to display next to the schedule name.
Day	Select the days of the week for the custom schedule.
Start	Select the schedule start time.
End	Select the schedule end time.

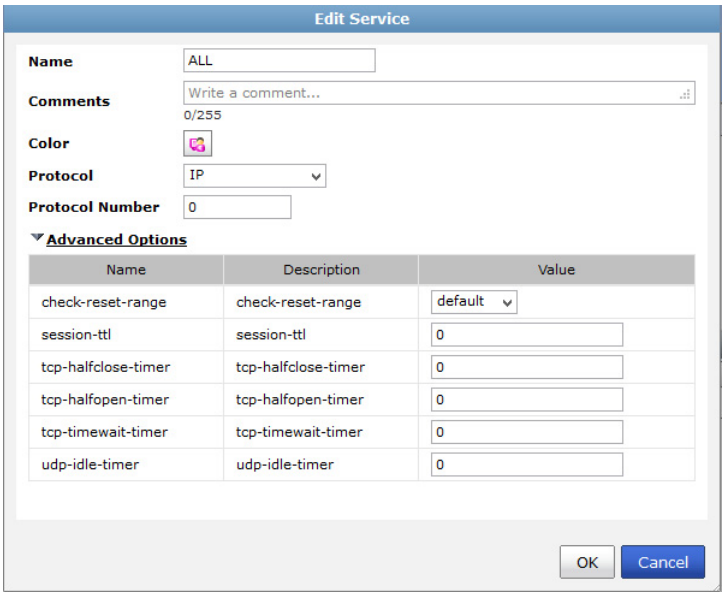
4. Select *OK* to save the schedule. The custom schedule will be added to *Objects* > *Firewall Objects* > *Schedule*.

Edit the policy service:

1. Select *NAT46 Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Service* column and select *Edit* in the menu.

   The *Edit Service* dialog box is displayed.

Figure 199: Edit Service



3. Configure the following settings:

Name	Edit the service name as required.
Comments	Enter an optional comment.
Color	Select the icon to select an custom icon to display next to the service name.
Protocol	Select the protocol from the drop-down list. Select one of the following: *TCP/UDP/SCTP, ICMP, ICMP6,* or *IP*.

IP/FQDN	Enter the IP or FQDN. *Note:* This menu item is available when *Protocol* is set to *TCP*/*UDP*/*SCTP*. You can then define the protocol, source port and destination port in the table.
Type	Enter the type in the text field. *Note:* This menu item is available when *Protocol* is set to *ICMP* and *ICMP6*.
Code	Enter the code in the text field. *Note:* This menu item is available when *Protocol* is set to *ICMP* and *ICMP6*.
Protocol Number	Enter the protocol number in the text field. *Note:* This menu item is available when *Protocol* is set to *IP.*
Advanced Options	For more information on advanced option, see the *FortiOS 5.0 CLI Reference*.
check-reset-range	Configure ICMP error message verification. • `disable` — The FortiGate unit does not validate ICMP error messages. • `strict` — If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) | TCP(C,D) header, then if FortiOS can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If is enabled the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the `anti-replay` option checks packets. • `default` — Use the global setting defined in `system global`. *Note:* This field is available when `protocol` is `TCP/UDP/SCTP`. *Note:* This field is not available if `explicit-proxy` is enabled.
session-ttl	Enter the default session timeout in seconds. The valid range is from 300 - 604 800 seconds. Enter `0` to use either the per-policy session-ttl or per-VDOM session-ttl, as applicable. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`
tcp-halfclose-timer	Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is from 1 to 86400 seconds. Enter `0` to use the global setting defined in `system global`. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`.

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

4. Select *OK* to save the service. The custom service will be added to *Objects* > *Firewall Objects* > *Service*.

To edit the policy action:

1. Select *NAT46 Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Action* column.
3. Select either *Accept* or *Deny* in the menu.

To edit policy logging:

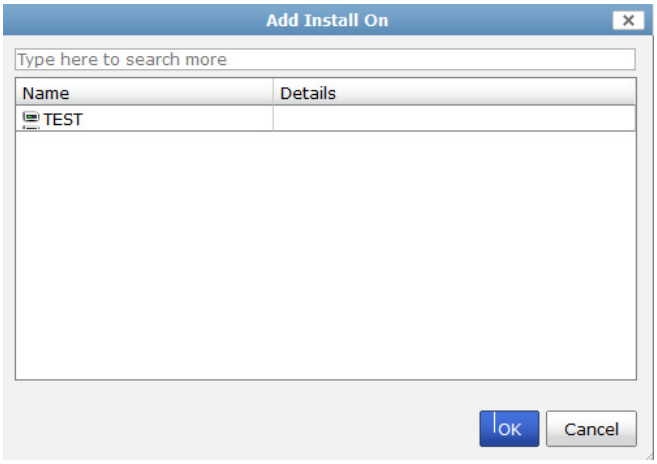
1. Select *NAT46 Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Log* column.
3. You can select to enable or disable logging in the menu.

To edit the installation target:

1. Select *NAT46 Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Install On* column and select *Add Object(s)* in the menu.

   The *Add Install On* dialog box is displayed.

Figure 200: Add Install On



3. Select the installation targets from the list and select *OK*. To edit the installation targets, select the *Installation* tab in the Policy Package tab bar and select *Edit Targets* in the toolbar.

NAT64 Policy

Use NAT64 policies to perform network address translation (NAT) between an internal IPv6 network and an external IPv4 network. The NAT64 Policy tab allows you to create, edit, delete, and clone NAT64 policies.



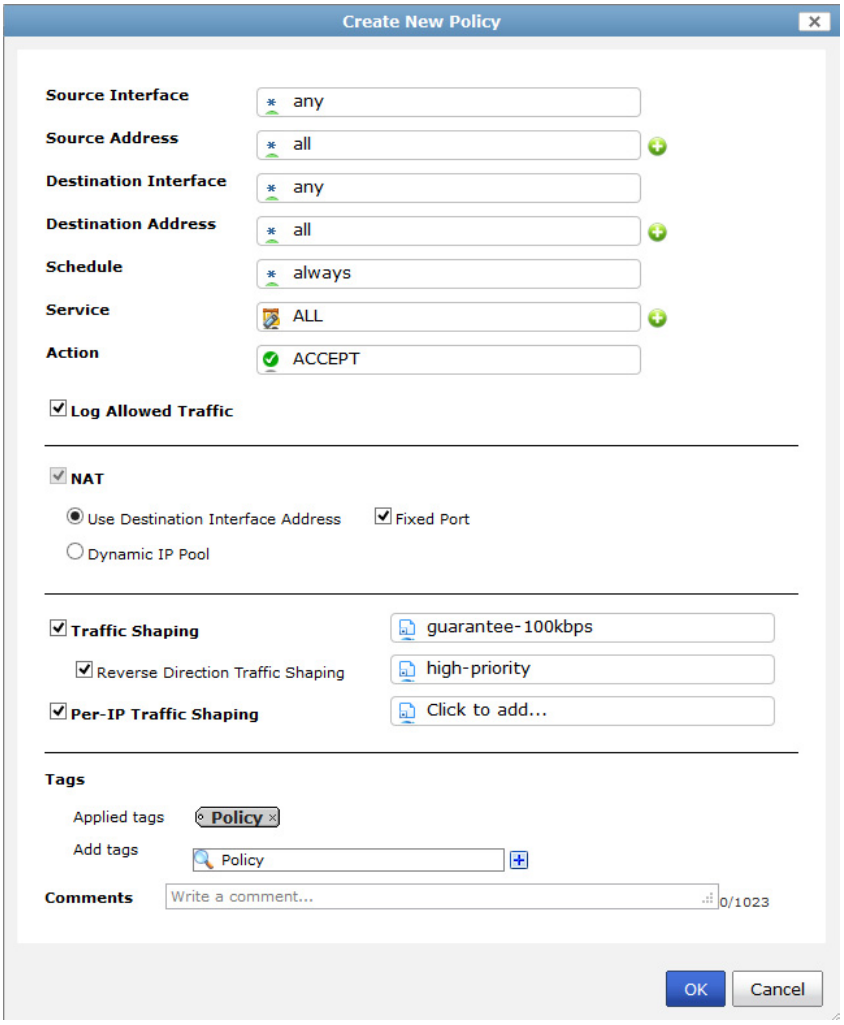
Select *Display Options* in the *Policy & Objects* tab, and toggle the *NAT64 Policy* switch to display this option in the Policy Package tab bar.

To create a NAT64 policy:

1. Select the ADOM from the drop-down list in the toolbar.
2. Select the policy package where you are creating the new NAT64 policy from the tree menu.
3. Select *NAT64 Policy* in the policy toolbar.
4. Right-click on the sequence number of a current policy, or in an empty area of the content pane and select *Create New* from the pop-up menu.

   The *Create New Policy* dialog box opens.

Figure 201:NAT 64 Policy



5. Configure the following settings:

Source Interface	Select the source interface from the drop-down list.
Source Address	Select the source address from the drop-down list. You can select to create a new address or address group in the *Source Address* dialog box.
Destination Interface	Select the destination interface from the drop-down list.
Destination Address	Select the destination address from the drop-down list. You can create a new address or address group in the *Add Destination Address* dialog box.
Schedule	Select a schedule or schedules for the policy. Schedules can also be created by selecting *Create New* in the dialog box. See "Create a new object" on page 354 for more information.
Service	Select the service from the drop-down list. You can create a new service or service group in the *Add Service* dialog box.

Action	Select an action for the policy to take, whether *ACCEPT* or *DENY*. When *Action* is set to *Accept*, you can configure *NAT* and *Traffic Shaping*.
Log Allowed Traffic **Log Violation Traffic**	Select to log allowed traffic/violation traffic. This setting is dependent on the *Action* setting.
NAT	NAT is enabled by default for this policy type.
Use Destination Interface Access	Select to use the destination interface address.
Fixed Port	Select to enable fixed port.
Dynamic IP Pool	Select to enable dynamic IP pool and select the dynamic IP pool from the drop-down list.
Traffic Shaping	Select to enable traffic shaping and select a default or custom traffic shaper object from the drop-down list.
Reverse Direction Traffic Shaping	Select to enable reverse direction traffic shaping and select a default or custom traffic shaper object from the drop-down list.
Per-IP Traffic Shaping	Select to enable per-IP traffic shaping and select the related object from the drop-down list.
Tags	You can add tags for tag management. Enter a tag in the text field and select the plus (+) icon to apply the tag to the policy.
Comments	Enter optional comments for the policy.

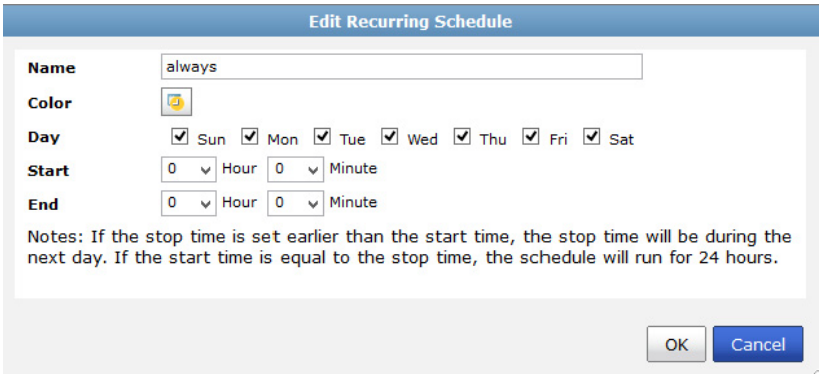
6. Select *OK* to save the policy.

Edit the policy schedule:

1. Select *NAT64 Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Schedule* column and select *Edit* in the menu.

   The *Edit Recurring Schedule* dialog box is displayed.

Figure 202: Edit Recurring Schedule



3. Configure the following settings:

Name	Edit the schedule name as required.
Color	Select the icon to select an custom icon to display next to the schedule name.
Day	Select the days of the week for the custom schedule.
Start	Select the schedule start time.
End	Select the schedule end time.

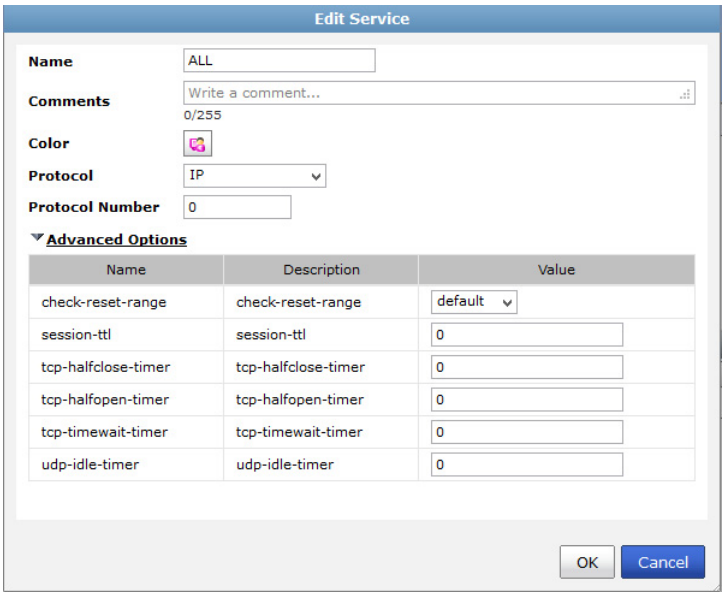
4. Select *OK* to save the schedule. The custom schedule will be added to *Objects* > *Firewall Objects* > *Schedule*.

Edit the policy service:

1. Select *NAT64 Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Service* column and select *Edit* in the menu.

   The *Edit Service* dialog box is displayed.

Figure 203: Edit Service



3. Configure the following settings:

Name	Edit the service name as required.
Comments	Enter an optional comment.
Color	Select the icon to select an custom icon to display next to the service name.
Protocol	Select the protocol from the drop-down list. Select one of the following: *TCP/UDP/SCTP, ICMP, ICMP6,* or *IP*.

IP/FQDN	Enter the IP or FQDN. *Note:* This menu item is available when *Protocol* is set to *TCP/UDP/SCTP*. You can then define the protocol, source port and destination port in the table.
Type	Enter the type in the text field. *Note:* This menu item is available when *Protocol* is set to *ICMP* and *ICMP6*.
Code	Enter the code in the text field. *Note:* This menu item is available when *Protocol* is set to *ICMP* and *ICMP6*.
Protocol Number	Enter the protocol number in the text field. *Note:* This menu item is available when *Protocol* is set to *IP.*
Advanced Options	For more information on advanced option, see the *FortiOS 5.0 CLI Reference*.
check-reset-range	Configure ICMP error message verification. • `disable` — The FortiGate unit does not validate ICMP error messages. • `strict` — If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) | TCP(C,D) header, then if FortiOS can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If is enabled the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the `anti-replay` option checks packets. • `default` — Use the global setting defined in `system global`. *Note:* This field is available when `protocol` is `TCP/UDP/SCTP`. *Note:* This field is not available if `explicit-proxy` is enabled.
session-ttl	Enter the default session timeout in seconds. The valid range is from 300 - 604 800 seconds. Enter `0` to use either the per-policy session-ttl or per-VDOM session-ttl, as applicable. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`
tcp-halfclose-timer	Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is from 1 to 86400 seconds. Enter `0` to use the global setting defined in `system global`. *Note:* This is available when `protocol` is `TCP/UDP/SCTP`.

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

4. Select *OK* to save the service. The custom service will be added to *Objects* > *Firewall Objects* > *Service*.

To edit the policy action:

1. Select *NAT64 Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Action* column.
3. Select either *Accept* or *Deny* in the menu.

To edit policy logging:

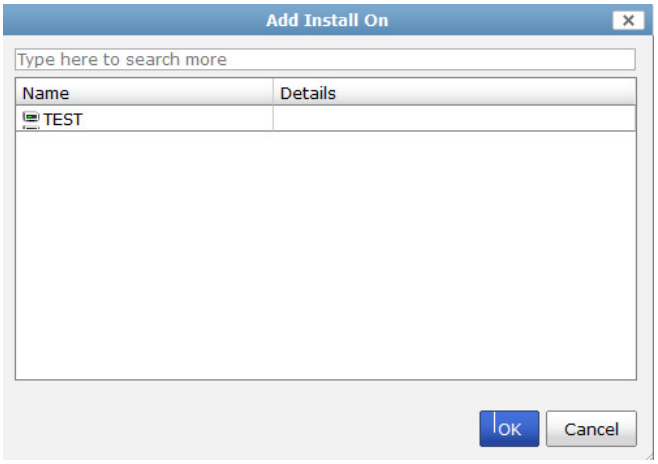
1. Select *NAT64 Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Log* column.
3. You can select to enable or disable logging in the menu.

To edit the installation target:

1. Select *NAT64 Policy* in the policy toolbar.
2. Select the policy in the table and right-click the *Install On* column and select *Add Object(s)* in the menu.

   The *Add Install On* dialog box is displayed.

Figure 204: Add Install On



3. Select the installation targets from the list and select *OK*. To edit the installation targets, select the *Installation* tab in the Policy Package tab bar and select *Edit Targets* in the toolbar.

Insert a policy

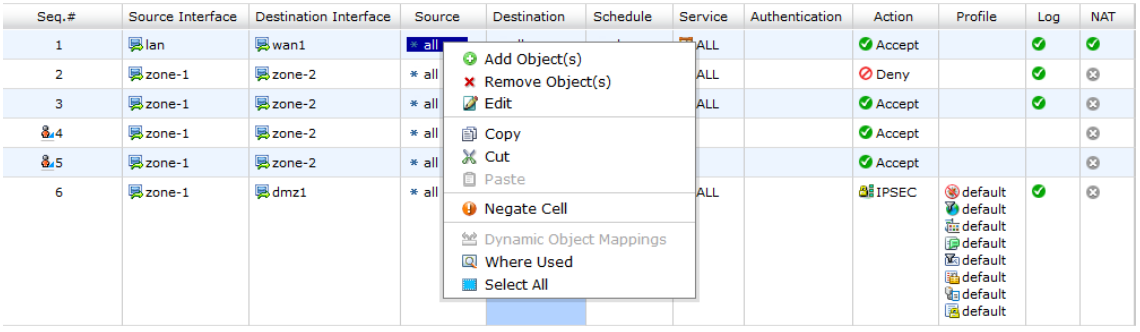
Generic policies can be inserted above or below the currently selected policy by right-clicking within the sequence number cell and selecting *Insert Policy* > *Above* or *Insert Policy* > *Below* from the pop-up menu.

Edit a policy

Policies can be edited by either right-clicking on the policy sequence number in the policy list and selecting *Edit* in the pop-up menu, or by double clicking on the sequence number. Both methods will open the *Edit Policy* dialog box.

Policies can also be edited in-line by right-clicking on either the cell that is to be edited or on the content within that cell. The right-click menu options vary depending on the cell that is selected. Values can be copied or cut and pasted into other policies, objects can be added, removed, edited, or deleted, and you can search for where a given object is used (see "Search where an object is used" on page 356 for more information).

Figure 205: Editing a policy



Clone a policy

To clone a policy, right-click in the policy sequence number cell and select *Clone* from the pop-up menu. The *Clone Policy* dialog box opens with all of the settings of the original policy. Edit the settings as required and select *OK* to create the clone.

Copy, cut, and paste a policy

Policies can be copied and cut using the requisite selection from the pop-up menu found by right-clicking in the policy sequence number cell.

When pasting a copied or cut policy, it can be inserted above or below the currently selected policy.

The pop-up menu also provides the option to *Cancel Copy/Cut* in the event that you need to undo the copy or cut that you just performed.

Delete a policy

To delete a policy, right-click in the policy sequence number cell and select *Delete* from the pop-up menu. Select *OK* in the confirmation dialog box to delete the policy.

Add a section

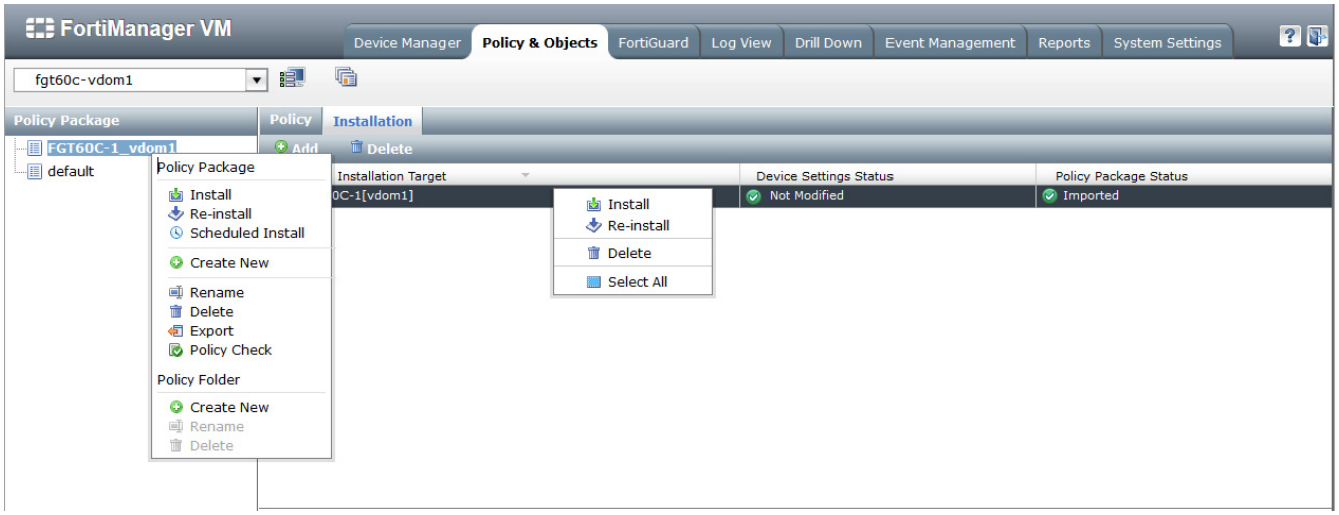
Sections can be used to help organize your policy list. Policies can also be appended to sections.

To add a section, right-clicking in the sequence number cell and select *Add Section* > *Above* or *Add Section* > *Below* to add a section either above or below the currently selected policy.

Installation page

The installation page allows you to view the installation target, device settings status, and policy package status, and edit installation targets for policy package installs. Go to the *Policy & Objects* tab, select the ADOM from the drop-down list, select the policy package in the tree menu, and select the *Installation* tab in the Policy Package tab bar.

Figure 206: Installation page



This page displays the following:

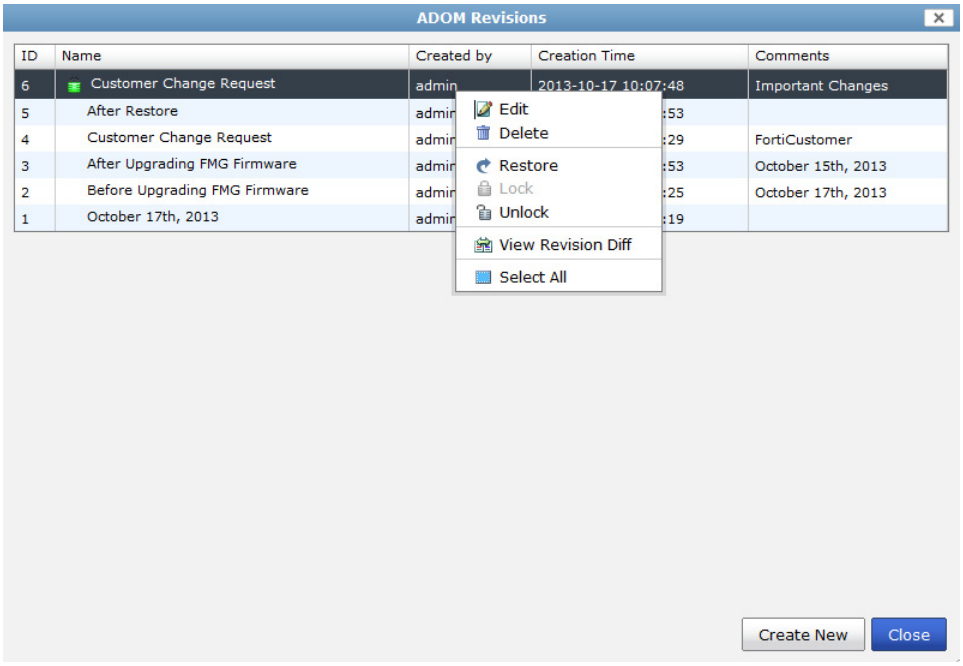
Add	Select to add installation targets (device/group) for the policy package selected.
Delete	Select to delete the selected entries from the installation target for the policy package selected.
Installation Target	The installation target and connection status.
Device Settings Status	The device settings synchronization status.
Policy Package Status	The policy package installation status.
Install	Right-click on an entry in the table and select *Install* in the menu to launch the *Install* wizard.
Re-install	Right-click on an entry in the table and select *Re-install* in the menu to perform a quick re-installation of the policy package to the installation targets.
Delete	Right-click on an entry in the table and select *Delete* in the menu to delete the selected entry.
Select All	Right-click on an entry in the table and select *Select ALL* in the menu to select all entries in the table. You can then select to re-install or delete the selected the entries.

ADOM revisions

ADOM revision history allows you to maintain a revision of the policy packages, objects, and VPN console settings in an ADOM. Revisions can be automatically deleted based on given variables, and individual revisions can be locked to prevent them being automatically deleted.

To configure ADOM revisions, select the *ADOM Revisions* button, , on the Policy & Objects tab.

Figure 207:ADOM revisions



This page displays the following:

ID	The ADOM revision identifier.
Name	The name of the ADOM revision. This field is user-defined when creating the ADOM revision. *Note:* A green lock icon will be displayed beside the ADOM revision name when you have selected *Lock this revision from auto deletion.*
Created by	The administrator that created the ADOM revision.
Creation Time	The ADOM revision creation date and time.
Comments	Optional comments entered in the *Description* field when the ADOM revision was created.
Create New	Select to create a new ADOM revision.
Close	Select to close the ADOM Revision dialog box and return to the Policy & Objects page.
Edit	Rick-click on a revision in the table and select *Edit* in the menu to edit the ADOM revision.

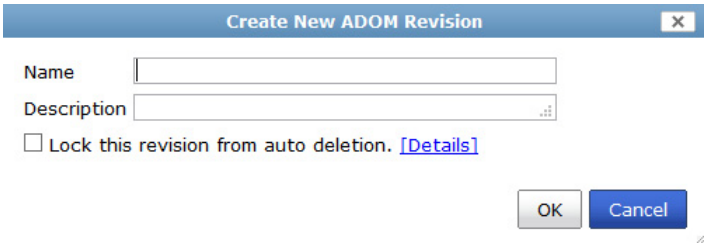
Delete	Rick-click on a revision in the table and select *Delete* in the menu to delete the ADOM revision. *Note:* When is *Lock this revision from auto deletion* selected, you are not able to delete the ADOM revision.
Restore	Rick-click on a revision in the table and select *Restore* in the menu to restore the ADOM revision. Restoring a revision will revert policy packages, objects and VPN console to the selected version. Select *OK* to continue.
Lock	Rick-click on a revision in the table and select *Lock* in the menu to lock this revision from auto deletion.
Unlock	Rick-click on a revision in the table and select *Unlock* in the menu to unlock this revision. When the ADOM revision is in an unlocked state, auto deletion will occur in accordance with your auto deletion settings.
View Revision Diff	Rick-click on a revision in the table and select *View Revision Diff* in the menu. The Summary page will be displayed. This page shows the revision differences between the selected revision and the current database.
Select All	Rick-click on a revision in the table and select *Select All* in the menu. You can then select to *Delete* all unlocked ADOM revisions.

To add a new ADOM revision:

1. Go to the Policy & Objects tab and select the *ADOM Revisions* button in the toolbar. The *ADOM Revisions* window opens.
2. Select *Create New*.

   The *Create New ADOM Revision* dialog box opens.

   Figure 208: Create new ADOM revision



3. Enter a name for the revisions in the *Name* field.
4. Optionally, enter a description of the revision in the *Description* field.
5. To prevent the revision from being automatically deleted, select *Lock this revision from auto deletion*.
6. To configure the automatic deletion of revisions, select *[Details]*. See "To configure automatic deletion:" on page 335.
7. Select *OK* to create the new ADOM revision.

To edit an ADOM revision:

1. Open the *ADOM Revisions* window and either double-click on the revision, or right-click on the revision and select *Edit* from the pop-up menu.

   The *Edit ADOM Revision* dialog box opens.

2. Edit the revision details as required, then select *OK* to apply your changes.

To delete ADOM revisions:

1. Open the *ADOM Revisions* window.
2. To delete a single revision, right-click on the revision and select *Delete* from the pop-up menu.

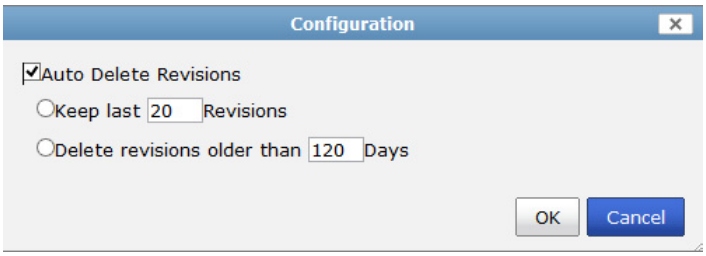
   To delete multiple revisions, use the Ctrl or Shift keys on your keyboard to select multiple revisions, or right-click on a revision and select Select All from the pop-up menu to select all of the revision. Then, right-click on any one of the selected revisions and select *Delete* from the pop-up menu.
3. Select *OK* in the confirmation dialog box to delete the selected revision or revisions.

To configure automatic deletion:

1. Open the *ADOM Revisions* window.
2. Right-click on any revision in the table and select *Edit* from the pop-up menu.
3. In the *Edit ADOM Revision* dialog box select *[Details]*.

   The *Configuration* dialog box opens.

   Figure 209:ADOM revision deletion configuration



4. To enable to automatic deletion of revisions, select *Auto Delete Revisions*.
5. Select one of the two available options for automatic deletion of revisions:
   - *Keep last x Revisions*: Only keep the entered numbered of revisions, deleting the oldest revision when a new revision is created.
   - *Delete revision older than x Days*: Delete all revisions that are older than the entered number of days.
6. Select *OK* to apply the changes, then select *OK* again in the *Edit ADOM Revision* dialog box.

To lock or unlock an ADOM revision:

1. Open the *ADOM Revisions* window.
2. Do one of the following:
   - Right-click on a revision in the table and select *Lock* or *Unlock* from the pop-up menu.
   - Edit the revision and select or deselect *Lock this revision from auto deletion* from the *Edit ADOM Revision* dialog box. See "To edit an ADOM revision:" on page 335.

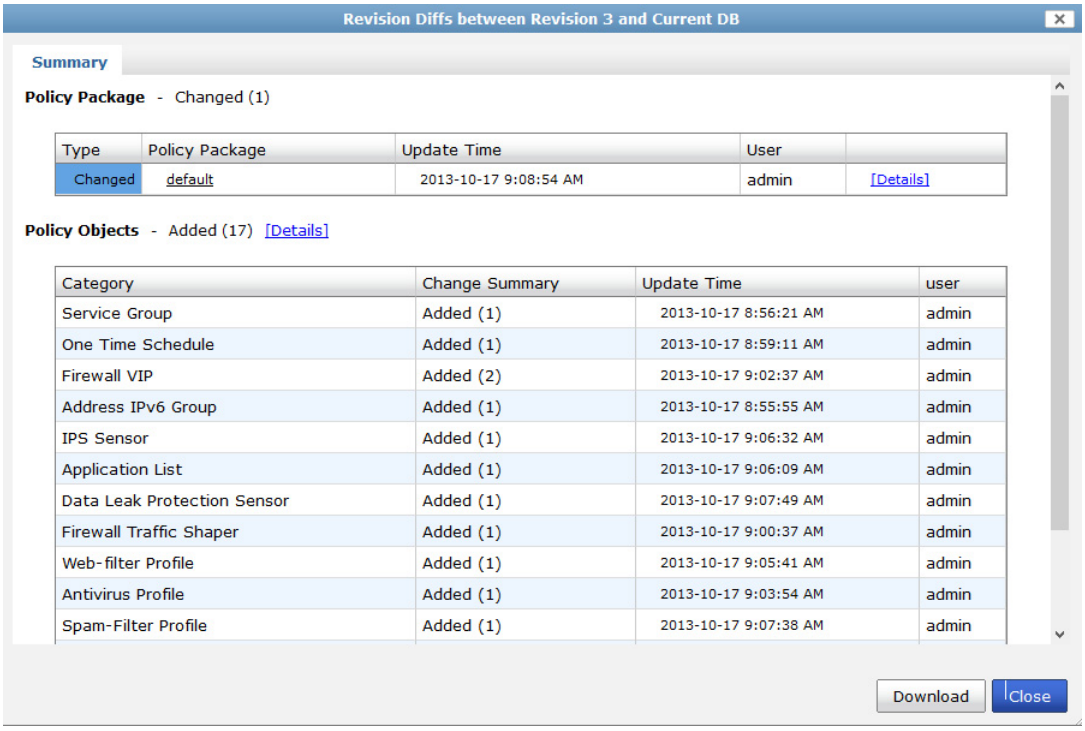
   The ADOM revision is locked.

To view ADOM revision diff:

1. Open the *ADOM Revisions* window.

2. Right-click on a revision in the table and select *View Revision Diff* from the pop-up menu. The *Summary* page will load.

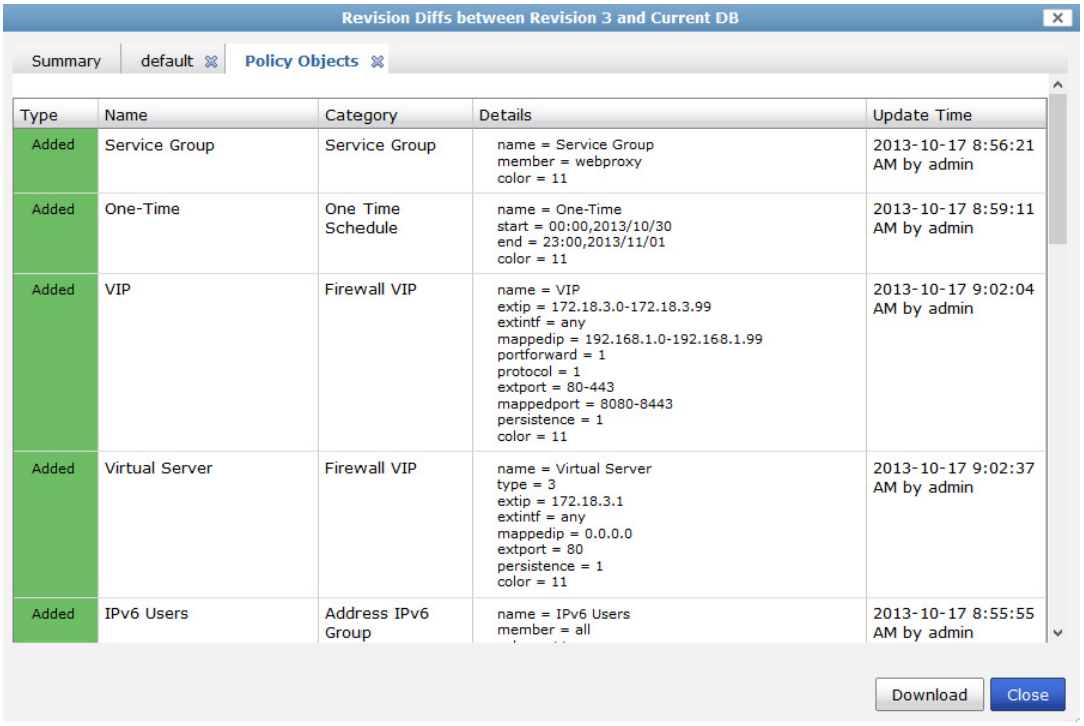
Figure 210:ADOM Revision Diff



This page displays all *Policy Package* and *Policy Object* changes between the revision selected and the current database.

3. Select *[Details]* to view all details on the changes made to policies and objects.

Figure 211: Details page



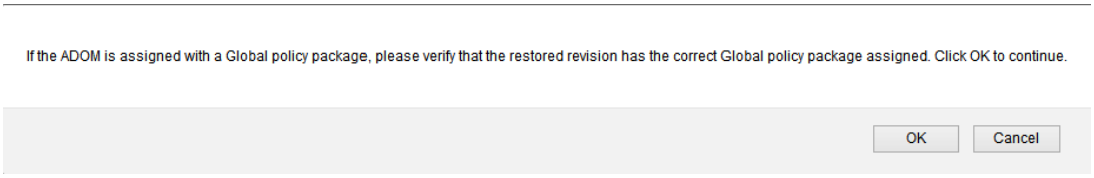
4. You can select to download this information as a `.csv` format file to your management computer.
5. Select *Close* to return to the Policy & Objects page.

To restore a previous ADOM revision:

1. Open the *ADOM Revisions* window.
2. Right-click on a revision in the table and select *Restore* from the pop-up menu.

   A confirmation dialog box will appear.

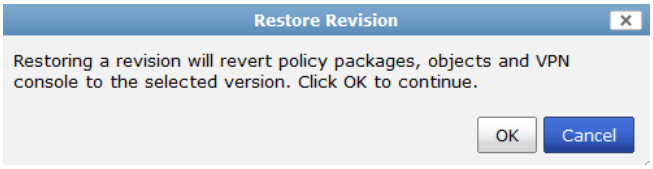
Figure 212: Restore confirmation



3. Select *OK* to continue.

   The *Restore Revision* dialog box will appear. Restoring a revision will revert policy packages, objects and VPN console to the selected version.

Figure 213: Restore Revision



4. Select *OK* to continue.

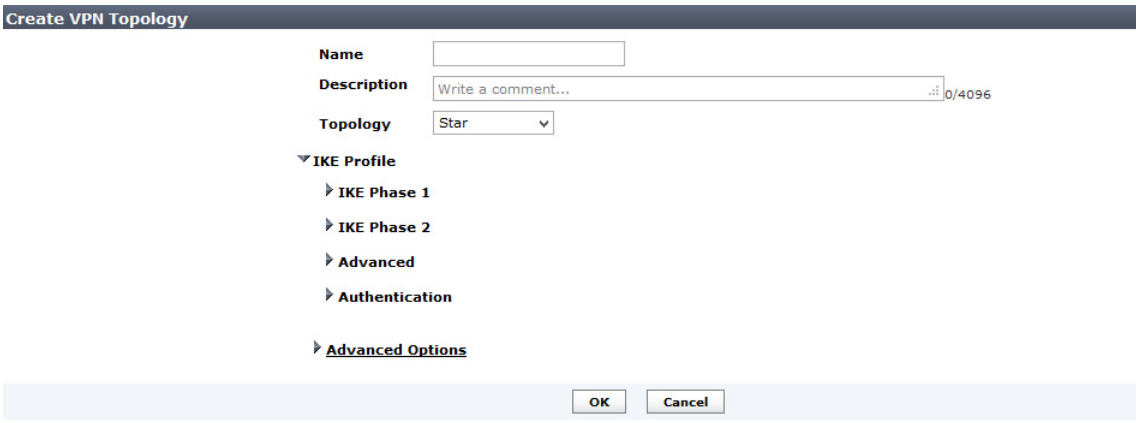
VPN Console

When Central VPN Console is selected for VPN Management when creating an ADOM, a VPN Console tree menu item will appear in the *Policy & Objects* tab under Policy Package. You can create VPN topologies on this page. Once you have configured a VPN topology and gateway, you can configure the related firewall policies, preview and install. For more information, see "Create a new policy or identity policy".

VPN topology

You can create full meshed, star, and dial up VPN topologies. Once you have created the topology, you can create the VPN gateway.

Figure 214: Create VPN Topology



Configure the following settings:

Name	Enter a name for the VPN topology.
Description	Enter an optional description.
Topology	Select the topology type from the drop-down list. Select one of: • *Full Meshed*: Each gateway has a tunnel to every other gateway. • *Star*: Each gateway has one tunnel to a central hub gateway. • *Dial up*: Some gateways, often mobile users, have dynamic IP addresses and contact the gateway to establish a tunnel.
IKE Profile	Define the IKE Profile. Configure IKE Phase 1, IKE Phase 2, Advanced settings, and Authentication settings.
IKE Phase 1	Define the IKE Phase 1 proposal settings.

1-Encryption Authentication **2-Encryption Authentication** **3-Encryption Authentication**	Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of three combinations. The remote peer or client must be configured to use at least one of the proposals that you define. Select one of the following symmetric-key encryption algorithms: • DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • 3DES: Triple-DES, in which plain text is encrypted three times by three keys. • AES128: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key. • AES192: A128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key. • AES256: A128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key. Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations: • MD5: Message Digest 5, the hash algorithm developed by RSA Data Security. • SHA1: Secure Hash Algorithm 1, which produces a 160-bit message digest. • SHA256: Secure Hash Algorithm 2, which produces a 256-bit message digest. To specify a third combination, use the Add button beside the fields for the second combination.
DH Group	Select one or more Diffie-Hellman groups from DH group 1, 2, 5 and 14. At least one of the DH Group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations. *Note:* Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.

Exchange Mode	Select either *Aggressive* or *Main (ID Protection).* The FortiGate unit and the remote peer or dialup client exchange phase 1 parameters in either Main mode or Aggressive mode. This choice does not apply if you use IKE version 2, which is available only for route-based configurations. In Main mode, the Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information In Aggressive mode, the Phase 1 parameters are exchanged in single message with authentication information that is not encrypted. Although Main mode is more secure, you must select Aggressive mode if there is more than one dialup Phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier local ID). Descriptions of the peer options in this guide indicate whether Main or Aggressive mode is required.
Key Life	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 172800 seconds.
Enable dead peer detection	Select this check box to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required. You can use this option to receive notification whenever a tunnel goes up or down, or to keep the tunnel connection open when no traffic is being generated inside the tunnel. For example, in scenarios where a dialup client or dynamic DNS peer connects from an IP address that changes periodically, traffic may be suspended while the IP address changes.
IKE Phase 2	Define the IKE Phase 2 proposal settings. *Note:* When you define phase 2 parameters, you can choose any set of phase 1 parameters to set up a secure connection for the tunnel and authenticate the remote peer. Auto Key configuration applies to both tunnel-mode and interface-mode VPNs.

1-Encryption Authentication **2-Encryption Authentication** **3-Encryption Authentication**	Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required. You need to select a minimum of one and a maximum of three combinations. The remote peer or client must be configured to use at least one of the proposals that you define. It is invalid to set both Encryption and Authentication to NULL. Select one of the following symmetric-key encryption algorithms: • NULL: Do not use an encryption algorithm. • DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • 3DES: Triple-DES, in which plain text is encrypted three times by three keys. • AES128: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key. • AES192: A128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key. • AES256: A128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key. Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations: • NULL: Do not use a message digest. • MD5: Message Digest 5, the hash algorithm developed by RSA Data Security. • SHA1: Secure Hash Algorithm 1, which produces a 160-bit message digest. • SHA256: Secure Hash Algorithm 2, which produces a 256-bit message digest. To specify a third combination, use the Add button beside the fields for the second combination.
DH Group	Select one or more Diffie-Hellman groups from DH group 1, 2, 5 and 14. At least one of the DH Group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations. *Note:* Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.
Enable replay detection	Select to enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.

Enable perfect forward secrecy (PFS)	Select to enable or disable perfect forward secrecy (PFS). Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.
Key Life	Enter the PFS key life. Select *Second, Kbytes,* or *Both* from the drop-down list and enter the value in the text field.
Enable autokey keep alive	Select to enable or disable autokey keep alive. The phase 2 SA has a fixed duration. If there is traffic on the VPN as the SA nears expiry, a new SA is negotiated and the VPN switches to the new SA without interruption. If there is no traffic, the SA expires and the VPN tunnel goes down. A new SA will not be generated until there is traffic. The Autokey Keep Alive option ensures that a new SA is negotiated even if there is no traffic so that the VPN tunnel stays up.
Enable auto-negotiate	Select to enable or disable auto-negotiation.
Advanced	
Enable NAT Traversal	Select the check box if a NAT device exists between the local FortiGate unit and the VPN peer or client. The local FortiGate unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared) to connect reliably.
NAT Traversal Keep-alive Frequency	If you enabled NAT-traversal, enter a keep-alive frequency setting (10-900 seconds).
Authentication	The FortiGate unit implements the Encapsulated Security Payload (ESP) protocol. Internet Key Exchange (IKE) is performed automatically based on pre-shared keys or X.509 digital certificates. As an option, you can specify manual keys. Interface mode, supported in NAT mode only, creates a virtual interface for the local end of a VPN tunnel.
Pre-shared Key	If you selected Pre-shared Key, 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. The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters. Alternatively, you can select to generate a random pre-shared key.
Certificates	If you selected Certificates, select the name of the server certificate that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. For information about obtaining and loading the required server certificate, see the *FortiOS User Authentication* guide.

Advanced Options	For more information on advanced option, see the *FortiOS 5.0 CLI Reference*.
fcc-enforcement	Select to enable or disable FCC enforcement.
ike-version	Select the version of IKE to use. This is available only if IPsec Interface Mode is enabled. For more information about IKE v2, refer to RFC 4306. IKE v2 is not available if *Exchange Mode* is *Aggressive*. When IKE Version is set to 2, Mode and XAUTH are not available.
localid-type	Select the local ID type from the drop-down list. Select one of: • auto: Select type automatically • fqdn: Fully Qualified Domain name • user-fqdn: User Fully Qualified Domain Name • keyid: Key Identifier ID • address: IP Address • asn1dn: ASN.1 Distinguished Name
negotiate-timeout	Enter the negotiation timeout value. The default is 30 seconds.

Once you have created your VPN topology, you can select to create a new managed gateway or external gateway for the topology.

VPN gateway

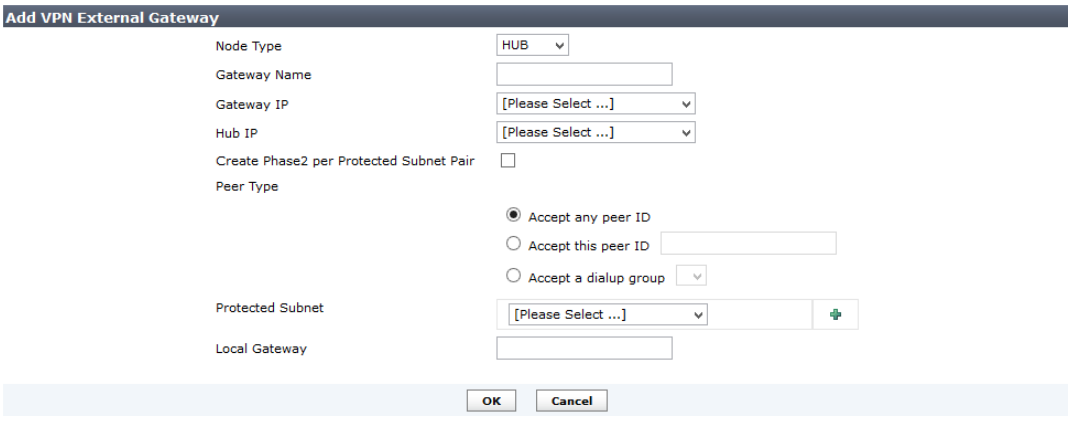
Once you have created the VPN topology, you can create a managed or external gateway. The settings on these pages are dependent on the VPN topology selected.

Create a VPN external gateway:

1. Select the VPN topology and select *Create New* > *External Gateway* in the toolbar.

   The *Add VPN External Gateway* page opens.

Figure 215: Add VPN External Gateway (Dial up topology)



2. Configure the following settings:

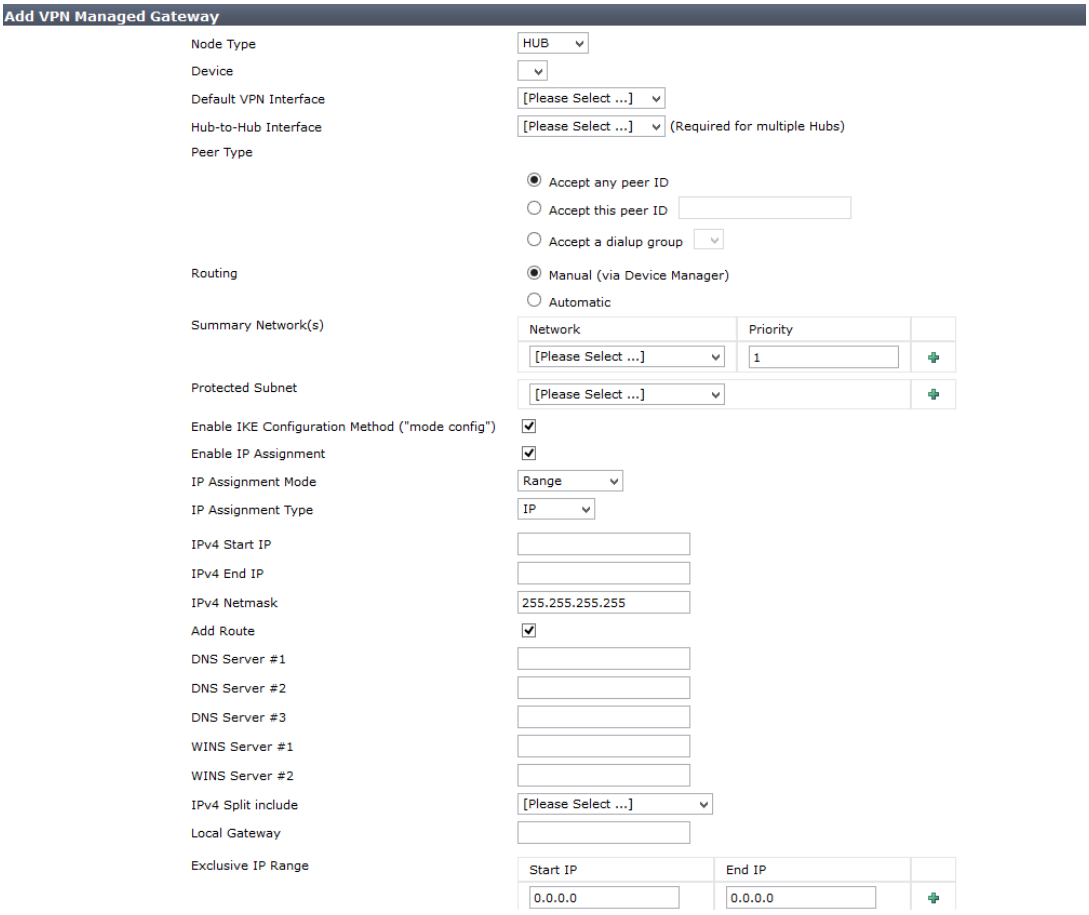
Node Type	Select either *HUB* or *Spoke* from the drop-down list. *Note:* This menu item is available when *Topology* is *Star* or *Dial up*.
Gateway Name	Enter the gateway name.
Gateway IP	Select the gateway IP address from the drop-down list.
Hub IP	Select the hub IP address from the drop-down list. *Note:* This menu item is available when *Topology* is *Star* or *Dial up* and *Node Type* is *HUB*.
Create Phase2 per Protected Subnet Pair	Select the checkbox to create a phase2 per protected subnet pair.
Peer Type	Select the peer type. Select one of the following: • Accept any peer ID • Accept this peer ID (enter the peer ID in the text field) • Accept a dialup group (select the group from the drop-down list) A Local ID is an alphanumeric value assigned in the Phase 1 configuration. The Local ID of a peer is called a Peer ID. The Local ID or peer ID can be used to uniquely identify one end of a VPN tunnel. This enables a more secure connection. Also if you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect. When you configure it on your end, it is your Local ID. When the remote end connects to you, they see it as your peer ID. If you are debugging a VPN connection, the Local ID is part of the VPN negotiations. You can use it to help troubleshoot connection problems. The default configuration is to accept all local IDs (peer IDs). If you have the Local ID set, the remote end of the tunnel must be configured to accept your Local ID. *Note:* This menu item is available when *Topology* is *Dial up*.
Protected Subnet	Select the address or address group from the drop-down list and select the plus (+) icon to add the entry. You can add multiple entries.
Local Gateway	Enter the local gateway in the text field.

3. Select *OK* to save the settings.

Create a VPN managed gateway:

1. Select the VPN topology and select *Create New* > *Managed Gateway* in the toolbar.
   The *Add VPN Managed Gateway* page opens.

Figure 216: Add VPN Managed Gateway (Dial up topology)



2. Configure the following settings:

Node Type	Select either *HUB* or *Spoke* from the drop-down list. *Note:* This menu item is available when *Topology* is *Star* or *Dial up*.
Device	Select the device from the drop-down list.
Default VPN Interface	Select the default VPN interface from the drop-down list.
Hub-to-Hub Interface	Select the hub-to-hub interface from the drop-down list. This field is mandatory for multiple hubs. *Note:* This menu item is available when *Topology* is *Star* or *Dial up* and *Node Type* is *HUB*.

Peer Type	Select the peer type. Select one of the following: • Accept any peer ID • Accept this peer ID (enter the peer ID in the text field) • Accept a dialup group (select the group from the drop-down list) *Note:* This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
Routing	Select either *Manual (via Device Manager)* or *Automatic*.
Summary Network(s)	Select the address or address group from the drop-down list, select the priority and select the plus (+) icon to add the entry. You can add multiple entries. *Note:* This menu item is available when *Topology* is *Star* or *Dial up* and *Node Type* is *HUB*.
Protected Subnet	Select the address or address group from the drop-down list and select the plus (+) icon to add the entry. You can add multiple entries.
Enable IKE Configuration Method ("mode config")	Select to enable IKE Configuration Method. *Note:* This menu item is available when *Topology* is *Dial up*.
Enable IP Assignment	Select to enable IP assignment. *Note:* This menu item is available when *Topology* is *Dial up*.
IP Assignment Mode	Select either Range or User Group from the drop-down list. *Note:* This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
IP Assignment Type	Select either IP or Subnet from the drop-down list. *Note:* This menu item is available when *Topology* is *Dial up*, *Node Type* is *HUB,* and *IP Assignment Mode* is *Range*
IPv4 Start IP	Enter the IPv4 start IP address. *Note:* This menu item is available when *Topology* is *Dial up*, *Node Type* is *HUB,* and *IP Assignment Mode* is *Range*
IPv4 End IP	Enter the IPv4 end IP address. *Note:* This menu item is available when *Topology* is *Dial up*, *Node Type* is *HUB,* and *IP Assignment Mode* is *Range*
IPv4 Netmask	Enter the IPv4 network mask. *Note:* This menu item is available when *Topology* is *Dial up*, *Node Type* is *HUB,* and *IP Assignment Mode* is *Range*.
Add Route	Select the checkbox to add a route for this entry. *Note:* This menu item is available when *Topology* is *Dial up*.

DNS Server #1	Enter the DNS server IP address to provide IKE Configuration Method to clients. *Note:* This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
DNS Server #2	Enter the DNS server IP address to provide IKE Configuration Method to clients. *Note:* This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
DNS Server #3	Enter the DNS server IP address to provide IKE Configuration Method to clients. *Note:* This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
WINS Server #1	Enter the WINS server IP address to provide IKE Configuration Method to clients. *Note:* This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
WINS Server #2	Enter the WINS server IP address to provide IKE Configuration Method to clients. *Note:* This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
IPv4 Split include	Select the address or address group from the drop-down list. *Note:* This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
Local Gateway	Enter the local gateway in the text field.
Exclusive IP Range	Enter the start IP and end IP and select the plus (+) icon to add the entry. You can add multiple entries. *Note:* This menu item is available when *Topology* is *Dial up* and *Node Type* is *HUB*.
Advanced Options	For more information on advanced option, see the *FortiOS 5.0 CLI Reference*.
authpasswd	Enter the XAuth client password for the FortiGate. *Note:* This field is available when `xauthtype` is set to client.
authusr	Enter the XAuth client user name for the FortiGate. *Note:* This field is available when `xauthtype` is set to client.

authusrgrp	Select the authentication user group from the drop-down list. *Note:* This field is available when xauthtype is set to auto, pap, or chap. When the FortiGate unit is configured as an XAuth server, enter the user group to authenticate remote VPN peers. The user group can contain local users, LDAP servers, and RADIUS servers. The user group must be added to the FortiGate configuration before the group name can be cross referenced.
banner	Enter the banner value. Specify a message to send to IKE Configuration Method clients. Some clients display this message to users. This is available if mode-cfg (IKE Configuration Method) is enabled.

dns-mode	Select either manual or auto from the drop-down list.
	• auto: Assign DNS servers in the following order:
	  • Servers assigned to interface by DHCP.
	  • Per-VDOM assigned DNS servers.
	  • Global DNS servers.
	• manual: Use DNS servers specified in DNS Server 1, DNS Server 2 etc.

domain	Enter the domain value.
public-ip	Enter the public IP value. Use this field to configure a VPN with dynamic interfaces. Define a `public-ip` value here, which is the dynamically assigned PPPoE address, which remains static and does not change over time. See "VPN Console supports NAT device with a public IP feature" on page 22 for more information.
unity-support	Select either enable or disable from the drop-down list.
xauthtype	Select the XAuth type from the drop-down list. Select one of: disable, client, pap, chap, or auto.

3. Select *OK* to save the settings

VPN security policies

Once you have defined the IP source and destination addresses, the phase 1 authentication parameters, and the phase 2 parameters, you must define the VPN security policies.

FortiGate unit VPNs can be policy-based or route-based. There is little difference between the two types. In both cases, you specify phase 1 and phase 2 settings. However there is a difference in implementation. A route-based VPN creates a virtual IPsec network interface that applies encryption or decryption as needed to any traffic that it carries. That is why route-based VPNs are also known as interface-based VPNs. A policy-based VPN is implemented through a special security policy that applies the encryption you specified in the phase 1 and phase 2 settings.

An IPsec security policy enables the transmission and reception of encrypted packets, specifies the permitted direction of VPN traffic, and selects the VPN tunnel. In most cases, a single policy is needed to control both inbound and outbound IP traffic through a VPN tunnel.

For a route-based VPN, you create two security policies between the virtual IPsec interface and the interface that connects to the private network. In one policy the virtual interface is the source. In the other policy the virtual interface is the destination. The Action for both policies is Accept. This creates bidirectional policies that ensure traffic will flow in both directions over the VPN.

For a policy-based VPN, one security policy enables communication in both directions. You must select IPSEC as the Action and then select the VPN tunnel you defined in the phase 1 settings. You can then enable inbound and outbound traffic as needed within that policy, or create multiple policies of this type to handle different types of traffic differently. For example HTTPS traffic may not require the same level of scanning as FTP traffic.

Defining policy addresses

A VPN tunnel has two end points. These end points may be VPN peers such as two FortiGate gateways. Encrypted packets are transmitted between the end points. At each end of the VPN tunnel, a VPN peer intercepts encrypted packets, decrypts the packets, and forwards the decrypted IP packets to the intended destination.

You need to define firewall addresses for the private networks behind each peer. You will use these addresses as the source or destination address depending on the security policy.

In general:

- In a gateway-to-gateway, hub-and-spoke, dynamic DNS, redundant-tunnel, or transparent configuration, you need to define a policy address for the private IP address of the network behind the remote VPN peer.
- In a peer-to-peer configuration, you need to define a policy address for the private IP address of a server or host behind the remote VPN peer.

Defining security policies

Security policies allow IP traffic to pass between interfaces on a FortiGate unit. You can limit communication to particular traffic by specifying source address and destination addresses. Then only traffic from those addresses will be allowed.

Policy-based and route-based VPNs require different security policies.

A policy-based VPN requires an IPsec security policy. You specify the interface to the private network, the interface to the remote peer and the VPN tunnel. A single policy can enable traffic inbound, outbound, or in both directions.

A route-based VPN requires an Accept security policy for each direction. As source and destination interfaces, you specify the interface to the private network and the virtual IPsec interface of the VPN. The IPsec interface is the destination interface for the outbound policy and the source interface for the inbound policy. One security policy must be configured for each direction of each VPN interface.

If the security policy, which grants the VPN connection is limited to certain services, DHCP must be included, otherwise the client will not be able to retrieve a lease from the FortiGate's (IPsec) DHCP server, because the DHCP request (coming out of the tunnel) will be blocked.

Before you define the IPsec policy, you must:

- Define the IP source and destination addresses.
- Specify the phase 1 authentication parameters.
- Specify the phase 2 parameters.

You must define at least one IPsec policy for each VPN tunnel. If the same remote server or client requires access to more than one network behind a local FortiGate unit, the FortiGate unit must be configured with an IPsec policy for each network. Multiple policies may be required to

configure redundant connections to a remote destination or control access to different services at different times.

To ensure a secure connection, the FortiGate unit must evaluate IPSEC policies before ACCEPT and DENY security policies. Because the FortiGate unit reads policies starting at the top of the list, you must move all IPsec policies to the top of the list. When you define multiple IPsec policies for the same tunnel, you must reorder the IPsec policies that apply to the tunnel so that specific constraints can be evaluated before general constraints.

When you define a route-based VPN, you create a virtual IPsec interface on the physical interface that connects to the remote peer. You create ordinary Accept security policies to enable traffic between the IPsec interface and the interface that connects to the private network. This makes configuration simpler than for policy-based VPNs, which require IPsec security policies.

For more information on IPsec VPN, see the IPsec VPN for FortiOS 5.0 chapter of the FortiOS Handbook. See “Create a new policy or identity policy” on page 291 for information on creating a VPN policy on your FortiManager.

Managing objects and dynamic objects

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

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

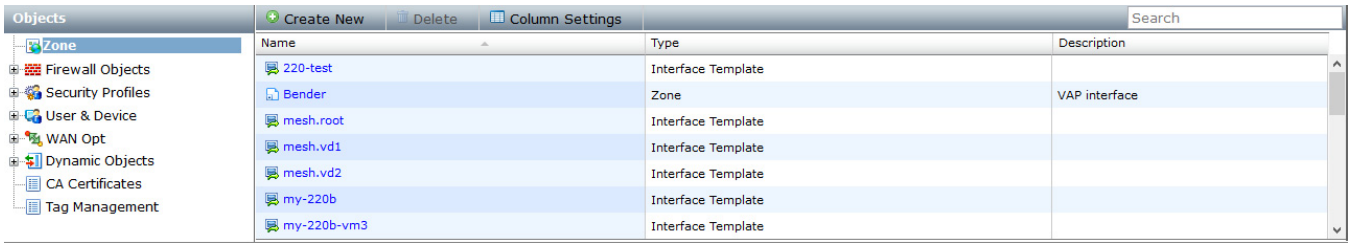
Dynamic objects are used to map a single logical object to a unique definition per device. Addresses, interfaces, virtual IPs, and an IP pool can all be addressed dynamically.



Not all policy and object options are enabled by default. To configure the enabled options, select the *Display Options* icon and select the display options in the dialog window. Select *OK* to save the setting.

Objects and dynamic objects are managed in lower frame of the *Policy & Objects* tab. The available objects varies depending on the specific ADOM selected.

Figure 217: Objects list



Objects can be dragged and dropped from the object frame into specific cells of a given policy. For example, an address object can be dragged into the source or destination cells of a policy. For more information see “Drag and drop objects” on page 357.

To view more information about an object in a policy, hover the pointer over the cell that contains that object. After one second, a tool tip will appear giving information about the object or objects in that cell.

Table 13: Objects and Global Objects

Objects Type	**Available Objects**	**Level**
Zone	• Zone Create a new zone.	ADOM and Global
Firewall Objects	• Address Create a new Address, Address Group, IPv6 Address, or IPv6 Address Group. • Service Create a new Service (Firewall or Explicit Proxy) or Service Group. • Schedule Create a new Recurring Schedule, One-time Schedule, or Schedule Group. • Traffic Shaper Create a new Shared Shaper or Per-IP Shaper. • Virtual IP Create a new IPv4 Virtual IP, IPv6 Virtual IP, NAT64 Virtual IP, NAT46 Virtual IP, IPv4 VIP Group, IPv6 VIP Group, NAT64 VIP Group, NAT 46 VIP Group, IP Pool, or IPv6 IP Pool. • Load Balance • Virtual Server • Real Server • Health Check Monitor • Web Proxy Create a new Web Proxy Forwarding Server.	ADOM and Global Note: Load Balance and Web Proxy are available at the ADOM level only.

Table 13: Objects and Global Objects (continued)

Objects Type	Available Objects	Level
Security Profiles	• AntiVirus Profile • Web Filter Profile • Application Sensor • IPS Sensor • Email Filter Profile • Data Leak Prevention Sensor • VoIP Profile • ICAP Profile • MMS Profile Create a new MMS Profile. (FortiCarrier only) • GTP Profile Create a new GTP Profile. (FortiCarrier only) • Advanced • Application List Create a Custom Application Signature. • Web Content Filter • Web URL Filter • Local Category • Rating Overrides Create a New Local Rating. • IPS Custom Signature Create a New Custom Signature. • Email List • File Filter • Detection List • ICAP Server Create a New ICAP Server. • Proxy Options Create new Proxy Options. • SSL/SSH Inspection Create New Deep Inspection Options. • Profile Group Create a new Profile Group. • SSL VPN Portal Create a new SSL-VPN Portal.	ADOM and Global

Table 13: Objects and Global Objects (continued)

Objects Type	Available Objects	Level
User & Device	• User Definition Create a New User. • User Group Create a New User Group. • Device Create a new Device or Device Group. • Remote Create a new LDAP, RADIUS, or TACACS+ Server. • PKI Create a New PKI User. • SMS Service Create a new SMS Server. • FortiToken Add a new FortiToken. • Single Sign-On Create a New RADIUS Single Sign-On Agent and Retrieve FSSO Agent.	ADOM and Global
WAN Opt	• Profile Create a new WAN Optimization Profile. • Peer Create a new WAN Optimization Peer. • Authentication Group Create a new Authentication Group.	ADOM and Global
Dynamic Objects	• Local Certificate Create a New Dynamic Local Certificate. • VPN Tunnel Create a New Dynamic VPN Tunnel.	ADOM only
CA Certificates	• CA Certificate Import and view CA Certificates.	ADOM only
Tag Management	• Tag Management Create a new Tag.	ADOM and Global

Lock an ADOM

If workspace is enabled, you must lock an ADOM prior to performing any management tasks on it. See "Lock an ADOM" on page 284 for instructions.

Create a new object

To create a new object:

1. Select the specific ADOM in which you are creating the object from the drop-down list in the toolbar, or select *Global* to create a global object.

   The objects list is displayed in lower frame.

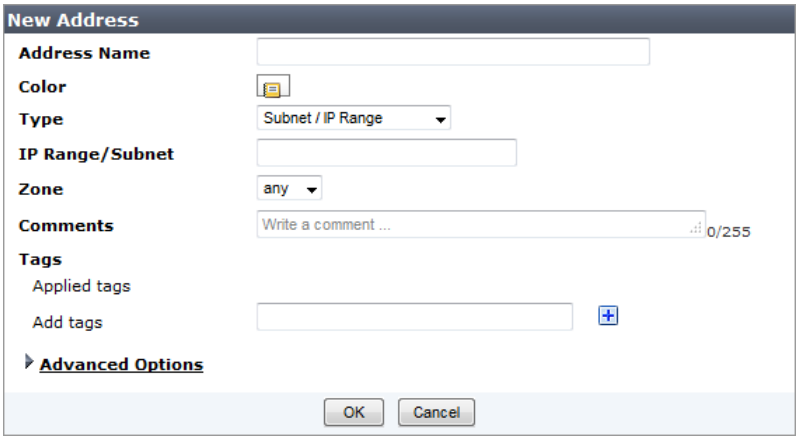
2. Select the object type that you will be creating. For example, view the firewall addresses by going to *Firewall Objects* > *Address*.

   The firewall address list is displayed in the lower content pane. The available address or address group lists are selectable on the lower content pane toolbar.

3. To create a new firewall address, select *Create New*, then select the type of address from the drop-down list. In this example, *Address* was selected.

   The *New Address* dialog window will open.

   Figure 218: Create new firewall address object



4. Enter the required information, depending on the object or object group selected, and then select *OK* to create the new object or object group.

Map a dynamic object

This example shows the basic steps for mapping an already created firewall address object. The same process is used for mapping other object types.

The devices and virtual domains to which a global object is mapped can also be viewed from the object list. See "To view dynamic object mappings:" on page 355.

To map a dynamic object:

1. Go to the *Device Manager* tab, select the ADOM containing the device you want to map the dynamic object to, then select the device from the device list in the content frame.

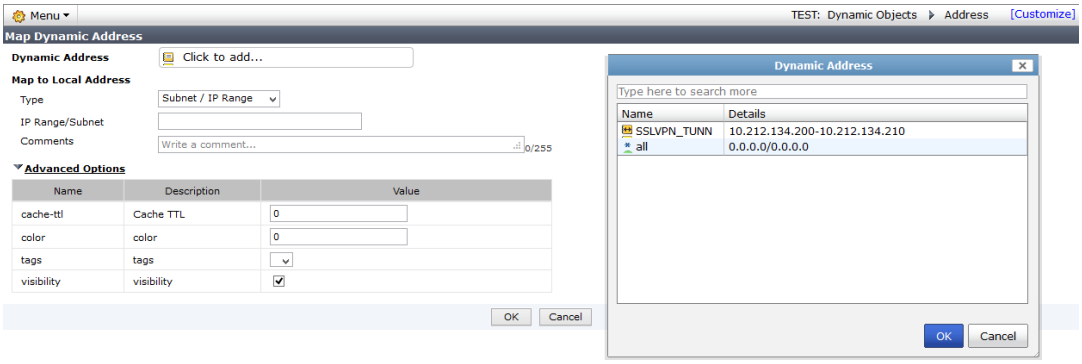
2. From the toolbar in the lower right content frame, select *Address.* Select *Create New* in the toolbar.

   The *Map Dynamic Address* dialog box will open.



The *Address* tab is not available by default. To add it, select the plus symbol on the right side of the dashboard toolbar, then select *Address* in the *Dynamic Objects* section of the *Customize Tabs* dialog box. See "View managed devices" on page 133.

Figure 219: Map Dynamic Address dialog box



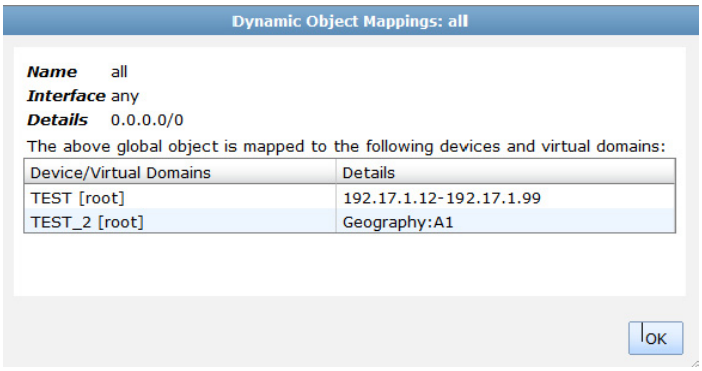
3. Select an address in the *Dynamic Address* field, then map that address to a local address. Select the type from the drop-down list and enter the dependent fields.
4. Optionally, add a description of the local address and adjust any required advanced settings, and then select *OK* to map the dynamic address object.

To view dynamic object mappings:

1. On the Policy & Objects tab, browse to the location of the object whose dynamic mappings you want to view in the object tree menu.
2. Right-click on the object in the object list and select *Dynamic Object Mappings*.

   The *Dynamic Object Mappings* dialog box opens, showing the details of the object and the devices and virtual domains to which it is mapped.

Figure 220: Dynamic object mappings



3. Select *OK* to close the dialog box.

Remove an object

To remove an object, browse to the object's location in the object tree menu, select the object in the object list, and either click on the *Delete* button, or right-click on the object name and select *Delete* from the pop-up menu.

Edit an object

To edit an object:

1. Browse to the location of the object that you want to edit in the object tree menu.
2. From the object list in the lower content pane, do one of the following:
   - Double-click on the name of the object to be edited
   - Right-click on the name of the object to be edited and select *Edit* from the pop-up menu.
3. Edit the information as required, and select *OK*.

Clone an object

If a new object that you are creating is similar to a previously created object, the new object can be created by cloning the previous object.

To clone an object:

1. Browse to the location of the object that is to be cloned in the object tree menu.
2. Right-click on the object or group and select *Clone* from the pop-up menu.

   The *Edit* dialog box opens.
3. Adjust the information as required, and then select *OK* to create the new object.

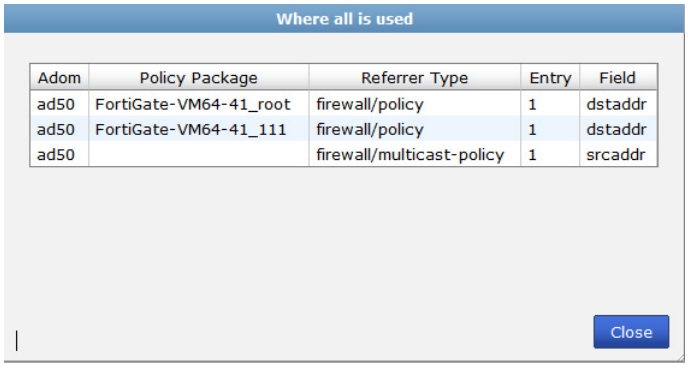
Search where an object is used

To determine where an object is being used:

1. Browse to the location of the object in the object tree menu or policy.
2. Right-click on the object or group and select *Where Used* from the pop-up menu.

   The *Where Used* dialog box opens and displays the locations where the selected object is used.

Figure 221: Where Used dialog box



3. Select *Close* to close the dialog box.

Search objects

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

To dynamically search objects:

1. Browse to the object type that you would like to search in the object tree menu.
2. In the search box on the right side lower content frame toolbar enter a search keyword.
3. The results of the search are updated as you type and displayed in the object list.

To search objects:

1. In the *Policy & Objects* tab enter *Search* keywords in the text field.
2. The results of the search are displayed in the content pane.

Drag and drop objects

Objects can be dragged and dropped from the object frame, or from other policies, into specific cells of a given policy. For example, an address object can be dragged into the source or destination cells of a policy.

One or more objects can be dragged at the same time. When dragging a single object a box beside the pointer will display the name of the object being dragged. When dragging multiple objects, the box beside the pointer will show a count of the number of objects that are being dragged.

The cells or columns that the object or objects can be dropped into will be highlighted in the policy package pane. After dropping the object or objects into a cell or column, the object will immediately appear in the cell as part of the policy, or in all the cells of that column.

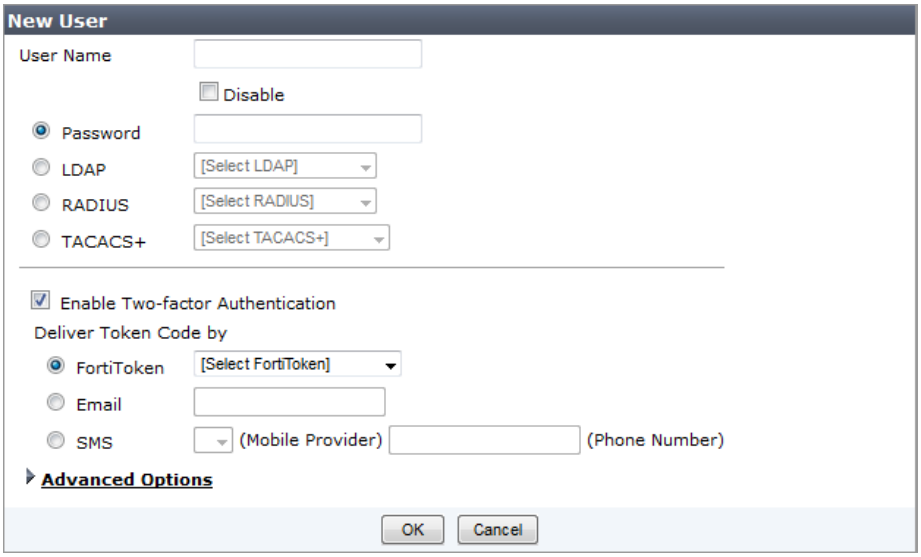
FortiToken configuration example

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

1. In the object tree menu, browse to *User & Device* > *FortiToken*.
2. Select *Create New* from the lower content frame toolbar.
3. Enter the serial number or serial numbers of the FortiToken unit or units and select *OK* to save the setting.

   Up to ten serial numbers can be entered.
4. Browse to *User & Device* > *Local User* to create a new user.
5. When creating the new user, select *Enable Two-factor Authentication,* and then select the FortiToken from the drop down menu.

Figure 222: New local user window



6. Browse to *User & Device* > *User Group*, create a new user group, and add the previously created user to this group.
7. Install a policy package to the FortiGate, as described previously.
8. On the FortiGate, select *User* > *FortiToken*. Select the FortiToken created in Step 1 and select *OK* to activate the FortiToken unit.

Log View

Logging and reporting can help you in determining what is happening on your network, as well as informing you of certain network activity, such as detection of a virus or IPsec VPN tunnel errors. Logging and reporting go hand in hand, and can become a valuable tool for information as well as helping to show others the activity that is happening on the network.

Your FortiManager device collects logs from managed FortiGate, FortiCarrier, FortiMail, FortiWeb devices and FortiClient endpoint agents. On FortiMail you can view history, event, antivirus, and email filter logs. On FortiWeb you can view event logs. On FortiGate and FortiCarrier you can view traffic, event, and security logs.

Traffic logs record the traffic that is flowing through your FortiGate unit. Since traffic needs firewall policies to properly flow through the unit, this type of logging is also referred to as firewall policy logging. Firewall policies control all traffic that attempts to pass through the FortiGate unit, between FortiGate interfaces, zones and VLAN sub-interfaces.

The event log records administration management as well as Fortinet device system activity, such as when a configuration has changed, admin login, or high availability (HA) events occur. Event logs are an important log file to record because they record Fortinet device system activity, which provides valuable information about how your Fortinet unit is performing. The FortiGate event logs includes *System*, *Router*, *VPN*, and *User* menu objects to provide you more granularity in viewing and searching log data.

Security logs (FortiGate) record all antivirus, web filtering, application control, intrusion prevention, email filtering, data leak prevention, and VoIP activity on your managed devices.



The logs displayed on your FortiManager are dependent on the device type logging to it. FortiGate, FortiCarrier, FortiMail, FortiWeb, and FortiClient logging is supported. ADOMs must be enabled to support FortiMail and FortiWeb logging.

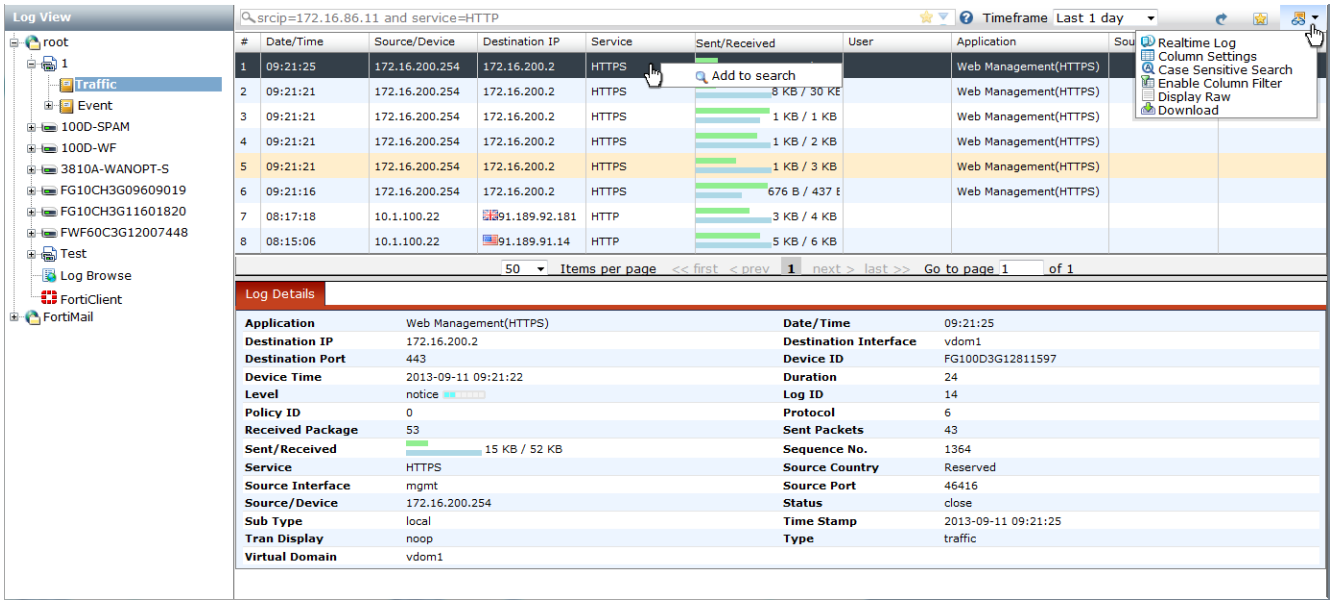
For more information on logging see the *Logging and Reporting for FortiOS v5.0 Handbook* at http://docs.fortinet.com/fgt/handbook/50/fortigate-loggingreporting-50.pdf.

The *Log View* tab shows log messages for connected devices, organized by ADOMs. You can also view, import, and export log files stored for a given device, and browse logs for all devices.

Viewing log messages

To view log messages, select the *Log View* tab and browse to the device whose logs you would like to view in the tree menu. You can view the traffic log, event log, or security log information per device or per log array. FortiMail and FortiWeb logs are found in the respective default ADOM. For more information on FortiGate raw logs, see the *FortiGate Log Message Reference*. For more information on FortiMail raw logs, see the *FortiMail Log Message Reference*.

Figure 223: Traffic log window (Formatted)



This page displays the following:

Search	Enter a search syntax. Select the drop-down icon to view *History*, *Bookmarks*, and *Filters*. Perform a search based on the filters. The filters available will vary based on device type and log type.
Star Icon	Select the star icon to save the search to favorites (bookmarks).
Question Mark Icon	Hover your mouse over this icon for example search syntax.
Timeframe	Select a time frame from the drop-down list. Select one of the following: Any time, Last 1 hour, Last 1 day, Last 7 days, or Last 30 days.
Refresh Icon	Refresh the log view.
Bookmarks Icon	Select the bookmarks icon to view all saved searches. Use the right-click menu to delete entries from bookmarks or paste the entry into the search field.

View Icon	When selecting the view icon a menu is displayed with the following options: • Realtime Log, Historical Log • Column Settings • Case Sensitive Search, Case Insensitive Search • Enable/Disable Column Filter • Display Raw, Display Formatted • Download
Realtime Log, Historical Log	Select this menu item to switch between *Realtime Log* and *Historical Log*. When *Realtime Log* is selected, logs displayed are updated in real time. When *Historical Log* is selected, you can search and download logs.
Column Settings	The default column settings and available fields will vary by device type. Select the *View* icon to change the column settings for the page you are currently viewing. This table provides details of the default columns.
Case Sensitive Search, Case Insensitive Search	Select this menu item to switch between case sensitive search and case insensitive search modes.
Enable/Disable Column Filter	Select to enable or disable column filters.
Log Details	Adjust the location and visibility of the *Log Details* frame. It can be hidden, or visible on the bottom or right side of the content pane. For more information, see "Log details" on page 369.
Pause/Resume Icon	Select to pause or resume log data. This option is only available when in the real time view.
Display Raw Display Formatted	Select either *Formatted* or *Raw*. Formatted log view displays log information by column. Raw log view provides a more granular level of log information, see Figure 224.
Download	Select to download the logs. Select the log file format in the drop-down list. Select either *Text* or *CSV* format. Select the checkbox to compress the log file with gzip. Select to download either the current page or all pages in the log.
Columns	Columns will be available, depending on the device type and log type selected in the tree menu. Select the *View* icon to change the column settings for the page you are currently viewing. This table provides details of the default columns.
Add to search	Right-click on a column value and select *Add to search* to search all logs that contain this value. You can select multiple values for search and save the search to favorites.

Traffic	Traffic log columns include the following information: • #: The log entry identifier. • Date/Time: The time the log was generated. Hover the mouse cursor over the entry to view the date and time. • Source/Device: The source device IP address. • Destination IP: The destination IP address and the country flag icon. Hover the mouse cursor over the flag icon to view the country information. • Service • Sent/Received: The number of packets sent and received in kB. Hover the mouse cursor over the entry to view the actual values. • User • Application • Source MAC • Security Action You can use the column filters to display specific logs. Alternatively, you can right-click on a log column entry to add that specific field to the search window and search all logs. You can view the log details in the lower content pane on the page.
Event > System	System log columns include the following information: • #: The log entry identifier. • Date/Time: The time the log was generated. Hover the mouse cursor over the entry to view the date and time. • Level: The logging level. Hover the house cursor over the entry to view the logging level. • Message: The log message content. • User You can use the column filters to display specific logs. Alternatively, you can right-click on a log column entry to add that specific field to the search window and search all logs. You can view the log details in the lower content pane on the page.
Event > VPN	VPN log columns include the following information: • #: The log entry identifier. • Date/Time: The time the log was generated. Hover the mouse cursor over the entry to view the date and time. • Level: The logging level. Hover the house cursor over the entry to view the logging level. • Action • Message: The log message content. • Status • VPN Tunnel You can use the column filters to display specific logs. Alternatively, you can right-click on a log column entry to add that specific field to the search window and search all logs. You can view the log details in the lower content pane on the page.

Event > User	User log columns include the following information: • #: The log entry identifier. • Date/Time: The time the log was generated. Hover the mouse cursor over the entry to view the date and time. • Level: The logging level. Hover the house cursor over the entry to view the logging level. • Action • Message: The log message content. • User • Status • Group You can use the column filters to display specific logs. Alternatively, you can right-click on a log column entry to add that specific field to the search window and search all logs. You can view the log details in the lower content pane on the page.
Event > Router	Router log columns include the following information: • #: The log entry identifier. • Date/Time: The time the log was generated. Hover the mouse cursor over the entry to view the date and time. • Level: The logging level. Hover the house cursor over the entry to view the logging level. • Message: The log message content. • IP You can use the column filters to display specific logs. Alternatively, you can right-click on a log column entry to add that specific field to the search window and search all logs. You can view the log details in the lower content pane on the page.
Event > Wireless	Wireless log columns include the following information: • #: The log entry identifier. • Date/Time: The time the log was generated. Hover the mouse cursor over the entry to view the date and time. • Level: The logging level. Hover the house cursor over the entry to view the logging level. • Action • Message: The log message content. • SSID • Channel You can use the column filters to display specific logs. Alternatively, you can right-click on a log column entry to add that specific field to the search window and search all logs. You can view the log details in the lower content pane on the page.

Security > Web Filter	Web Filter log columns include the following information: • #: The log entry identifier. • Date/Time: The time the log was generated. Hover the mouse cursor over the entry to view the date and time. • Source/Device: The source device IP address. • Destination IP: The destination IP address and the country flag icon. Hover the mouse cursor over the flag icon to view the country information. • Service • Host Name • Status • URL • Category Description • Sent/Received: The number of packets sent and received in kB. Hover the mouse cursor over the entry to view the actual values. You can use the column filters to display specific logs. Alternatively, you can right-click on a log column entry to add that specific field to the search window and search all logs. You can view the log details in the lower content pane on the page.
Security > Application Control	Application Control log columns include the following information: • #: The log entry identifier. • Date/Time: The time the log was generated. Hover the mouse cursor over the entry to view the date and time. • Level: The logging level. Hover the house cursor over the entry to view the logging level. • Message: The log message content. • User You can use the column filters to display specific logs. Alternatively, you can right-click on a log column entry to add that specific field to the search window and search all logs. You can view the log details in the lower content pane on the page.

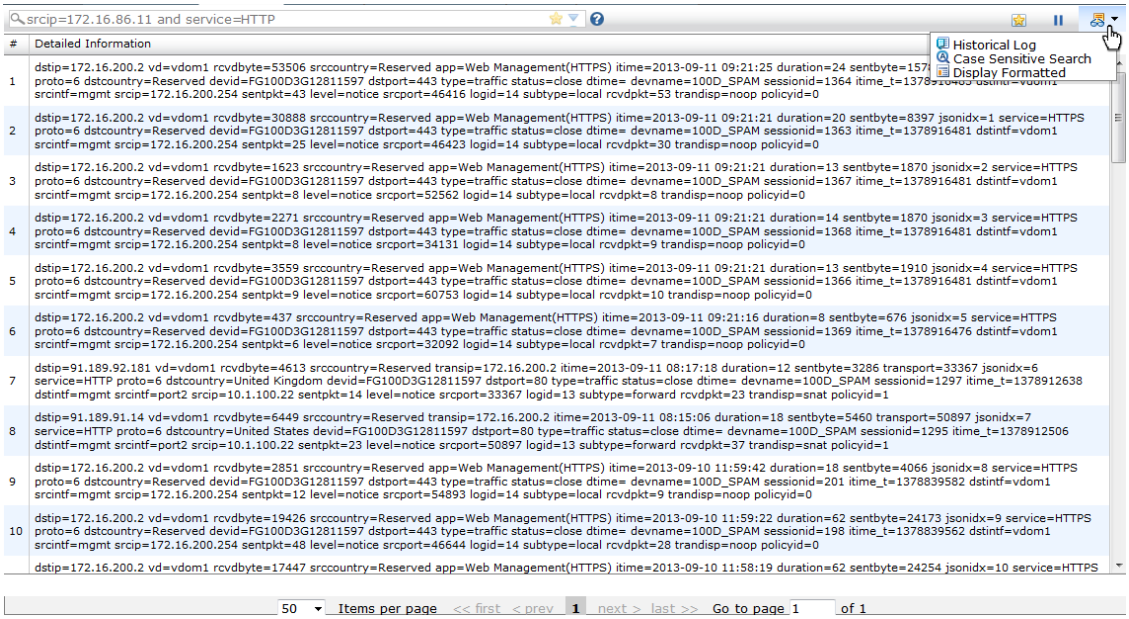
Security > Data Leak Prevention	Data Leak Prevention log columns include the following information: • #: The log entry identifier. • Date/Time: The time the log was generated. Hover the mouse cursor over the entry to view the date and time. • User • Source/Device: The source device IP address. • Service • URL • Action • File • Subject • Filter Index • Filter Type • DLP Extra Info You can use the column filters to display specific logs. Alternatively, you can right-click on a log column entry to add that specific field to the search window and search all logs. You can view the log details in the lower content pane on the page.
Security > Vulnerability Scan	Vulnerability Scan log columns include the following information: • #: The log entry identifier. • Date/Time: The time the log was generated. Hover the mouse cursor over the entry to view the date and time. • Destination IP: The destination IP address and the country flag icon. Hover the mouse cursor over the flag icon to view the country information. • Vulnerability • Severity • OS • Vulnerability Count • User You can use the column filters to display specific logs. Alternatively, you can right-click on a log column entry to add that specific field to the search window and search all logs. You can view the log details in the lower content pane on the page.

Content	Content log columns include the following information: • #: The log entry identifier. • Date/Time: The time the log was generated. Hover the mouse cursor over the entry to view the date and time. • Sub Type • Level: The logging level. Hover the house cursor over the entry to view the logging level. • Client: The client IP address. • Sent/Received: The number of packets sent and received in kB. Hover the mouse cursor over the entry to view the actual values. • Method • URL • To • From • Subject • FTP Command • File • Profile • Local • Remote • Status • Protocol • Action • Chat Message • File Name • File Size • Source/Device: The source device IP address. • Destination IP: The destination IP address and the country flag icon. Hover the mouse cursor over the flag icon to view the country information. • Phone • Host Name You can use the column filters to display specific logs. Alternatively, you can right-click on a log column entry to add that specific field to the search window and search all logs. You can view the log details in the lower content pane on the page.
Pages	Settings to adjust the number of logs listed per page and to browse through the pages of logs.
Log Details frame	Detailed information on the log message selected in the log message list. See “Log details” on page 369 for more information.

Depending on configuration and the device type, different logs will be available, such as traffic logs, event logs, and security logs.

Figure 224 shows the granular raw log details. When selecting to view raw logs you can view either real time or historical logs. You can download the log file in text or CSV format file.

Figure 224: Traffic log window (Raw)

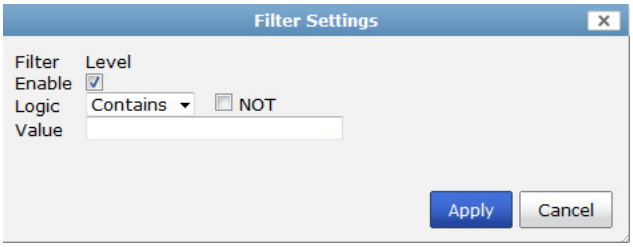


Customizing the log view

The columns in the log message list can be customized to show only relevant information in your preferred order.

For most columns, you can also filter data within the columns to include or exclude log messages which contain your specified text in that column. Most column headings contain a gray filter icon, which becomes green when a filter is configured and enabled. You can enable or disable column filters in the *View* menu.

Figure 225: Filter settings dialog box





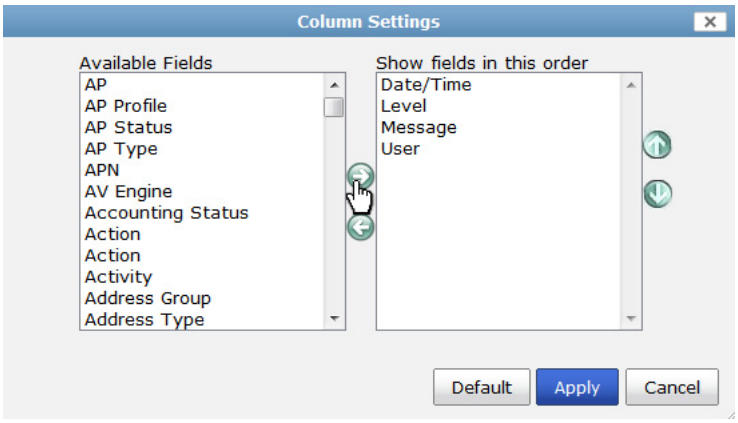
The available column settings will vary based on the device and log type selected. The filter settings will vary based on the column settings.

To display or hide columns:

1. Browse to the log message list you would like to customize
2. Select the *View* icon in the toolbar and select *Column Settings* in the menu.

   The *Column Settings* dialog box opens.

   Figure 226: Column settings dialog box



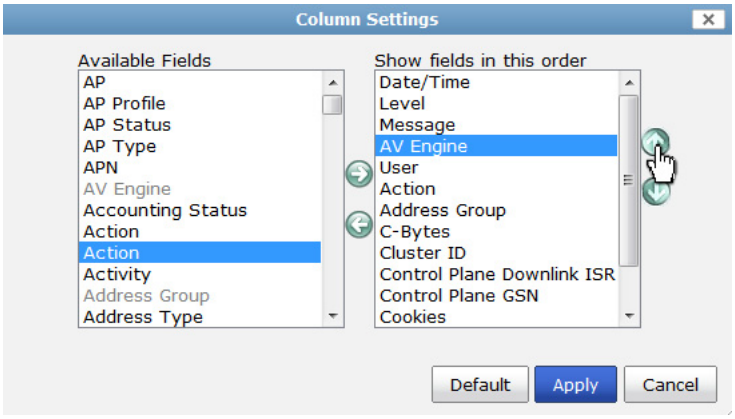
3. Select which columns to hide or display.
   - In the *Available Fields* area, select the names of individual columns you want to display, then select the single right arrow to move them to the *Show fields in this order* area.
   - In the *Show fields in this order* area, select the names of individual columns you want to hide, then select the single left arrow to move them to the *Available Fields* area.
   - To return all columns to their default displayed/hidden status, select the *Default* button.
4. Select *Apply* to apply the changes to the log message list.

To change the order of the columns:

1. Browse to the log message list you would like to customize
2. Select the *View* icon in the toolbar and select *Column Settings* in the menu.

   The *Column Settings* dialog box opens.

   Figure 227: Column settings dialog box



3. In the *Show fields in this order* area, select a column name whose order of appearance you want to change.

4. Select the up or down arrow to move the column in the ordered list.

   Placing a column name towards the top of the *Show fields in this order* list will move the column to the left side of the log message list.

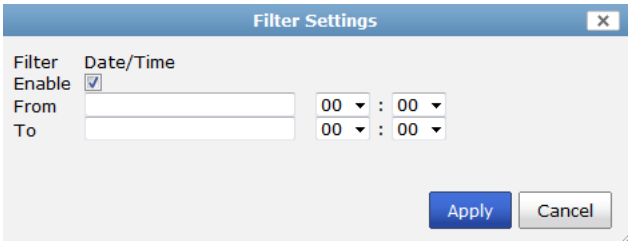
5. Select *Apply* to apply the changes to the log message list.

To filter log messages by column content:

1. Select the *View* icon in the toolbar and select *Enable Column Filter* in the menu.
2. In the heading of the column that you want to filter, select the filter icon to open the *Filter Settings* dialog box for that column. The *Filter Settings* dialog boxes are specific to the column you are filtering.

   The *Filter Settings* dialog box opens.

   Figure 228: Filter settings dialog box



3. Enter the requisite information to filter the selected column and then select *Apply*.

   The column's filter icon will turn green when the filter is enabled. Downloading the current view will only download the log messages that meet the current filter criteria.

Log details

Log details can be viewed for any of the collected logs. The fields available in the this pane cannot be edited or re-organized.

To view log details, select the log in the log message list. The log details frame will be displayed in the lower frame of the content pane.

Figure 229: Log details frame

Log Details

Application	Web Management(HTTPS)	**Date/Time**	09:21:25
Destination IP	172.16.200.2	**Destination Interface**	vdom1
Destination Port	443	**Device ID**	FG100D3G12811597
Device Time	2013-09-11 09:21:22	**Duration**	24
Level	notice	**Log ID**	14
Policy ID	0	**Protocol**	6
Received Package	53	**Sent Packets**	43
Sent/Received	15 KB / 52 KB	**Sequence No.**	1364
Service	HTTPS	**Source Country**	Reserved
Source Interface	mgmt	**Source Port**	46416
Source/Device	172.16.200.254	**Status**	close
Sub Type	local	**Time Stamp**	2013-09-11 09:21:25
Tran Display	noop	**Type**	traffic
Virtual Domain	vdom1		

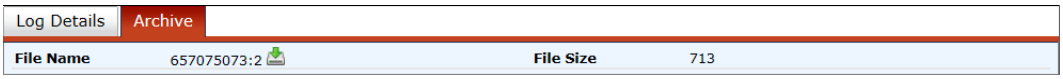


The details provided in the log detail frame will vary depending on the device and type of log selected.

Archive

The *Archive* tab is displayed next to the *Log Details* tab on the details frame when archived logs are available.

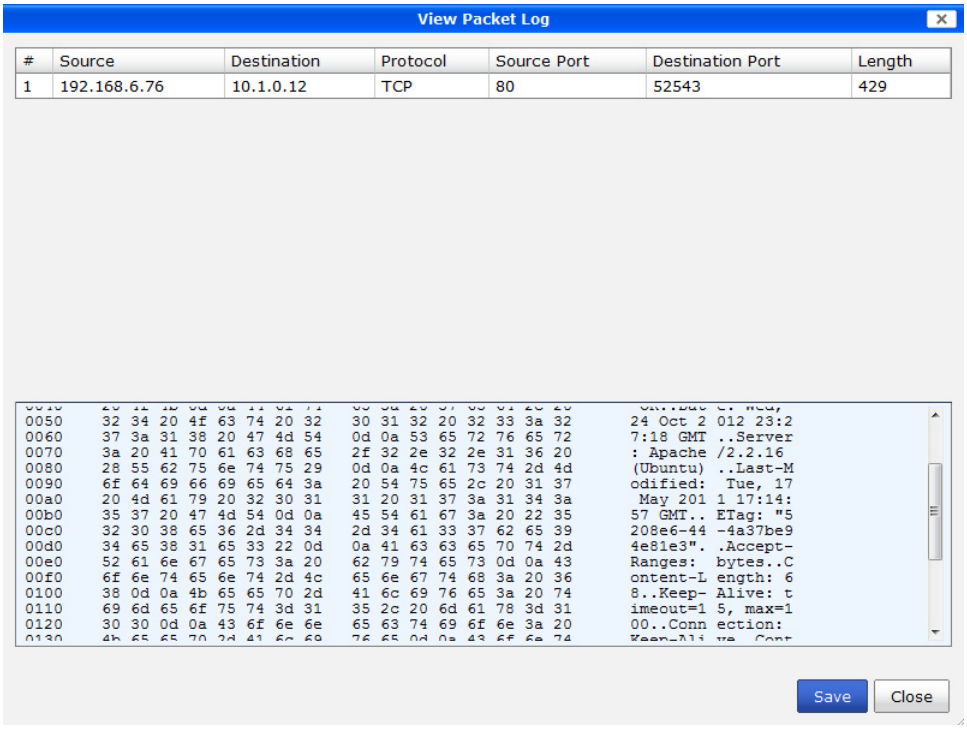
Figure 230: Log archive tab



The name and size of the archived log files are listed in the table. Selecting the download button next to the file name allows you to save the file to your computer.

Depending on the file type of the archived log file, the *View Packet Log* button may also be available next to the download button. Select this button to open the *View Packet Log* dialog box, which displays the path and content of the log file.

Figure 231: View packet log dialog box



Browsing log files

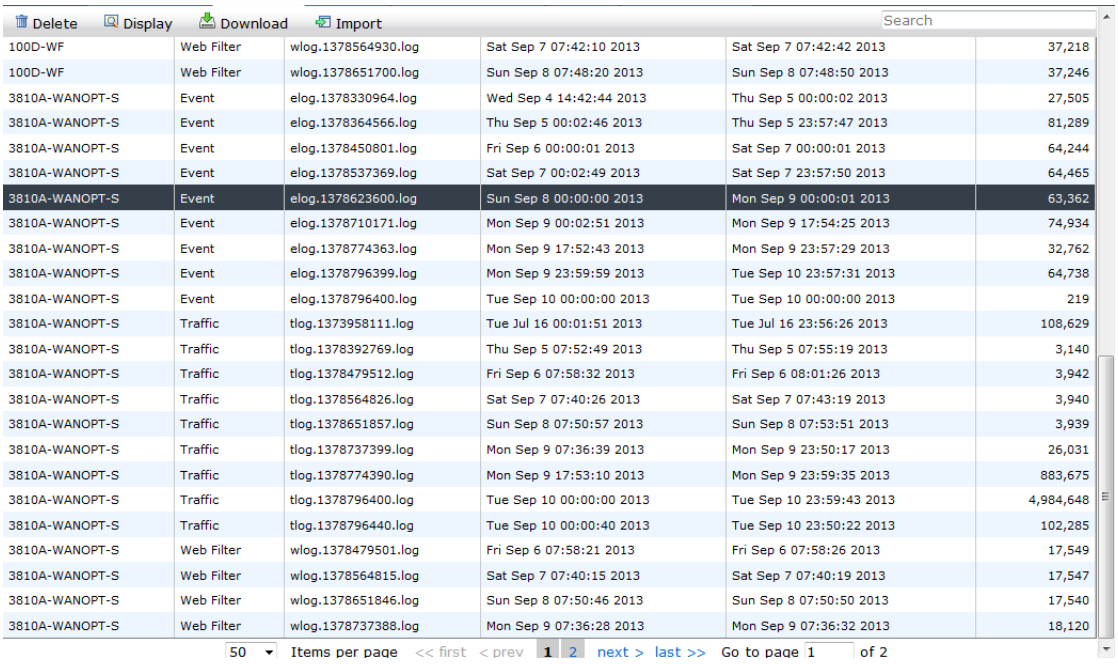
Go to *Log View* > *Log Browse* to view log files stored for devices. On this page you can display, download, delete, and import log files.

When a log file reaches its maximum size, or reaches the scheduled time, the FortiManager rolls the active log file by renaming the file. The file name will be in the form of xlog.N.log, where x is a letter indicating the log type and N is a unique number corresponding to the time the first log entry was received.

For information about setting the maximum file size and log rolling options, see "Configuring rolling and uploading of logs" on page 375.

If you display the log messages in formatted view, you can display and arrange columns and/or filter log messages by column contents. For more information, see "Customizing the log view" on page 367.

Figure 232: Log file list window

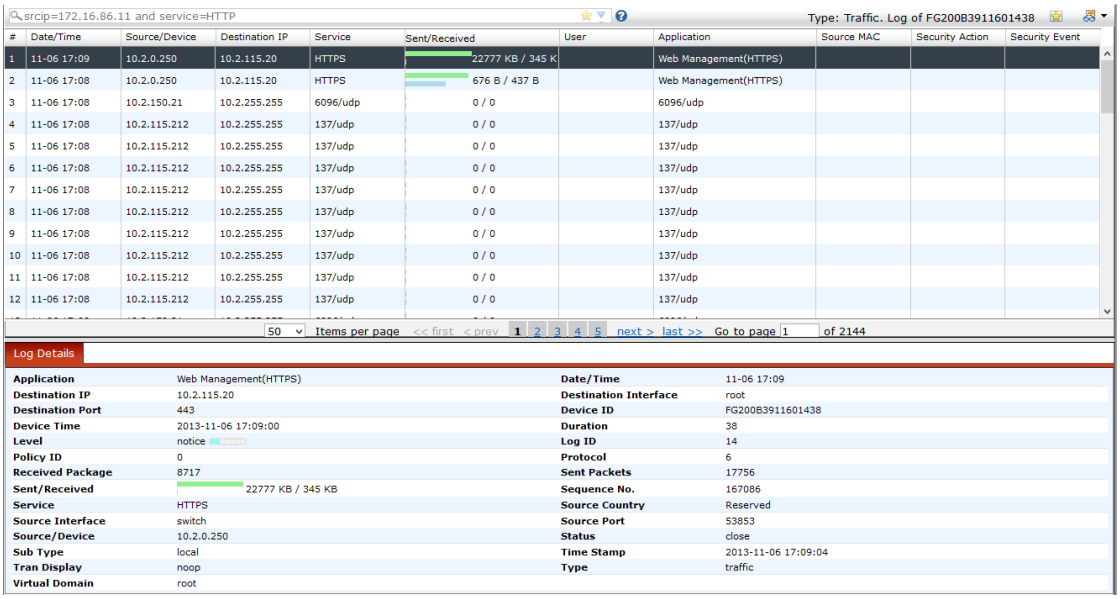


This page displays the following:

Delete	Mark the check box of the file whose log messages you want to delete, then select this button.
Display	Mark the check box of the file whose log messages you want to view, then select this button. For more information, see "Viewing log messages" on page 360
Download	Mark the check box of the log file that you want to download, select this button, then select a format for saving the log files: text (.txt), or comma-separated value (.csv). For more information, see "Downloading a log file" on page 374.

Import	Select to import log files. For more information about importing log files, see "Importing a log file" on page 373.
Search	Search the log files by entering a text value in the search window. For example, search log files by device serial number.
Columns	
Device	The device host name.
Type	The log type. For example, *Email Filter, Event, Traffic, Web Filter, Network Scan, Virus, Application Control, Data Leak Prevention*.
Log Files	A list of available log files for each device or device group. Select the group name to expand the list of devices within the group, and to view their log files. The current, or active, log file appears as well as rolled log files. Rolled log files include a number in the file name, such as `vlog.1267852112.log`. If you configure the FortiManager unit to delete the original log files after uploading rolled logs to an FTP server, only the current log will exist.
From	The start time when the log file was generated.
To	The end time when the log file was generated.
Size (bytes)	The size of the log file.
Items per page	Select to display 50, 100, or 500 log items per page.
First, Prev, 1, 2, .., Next Last	Navigate pages in the log browse page.
Go to page	Browse log file pages.

Figure 233: Display logs by serial number example



Importing a log file

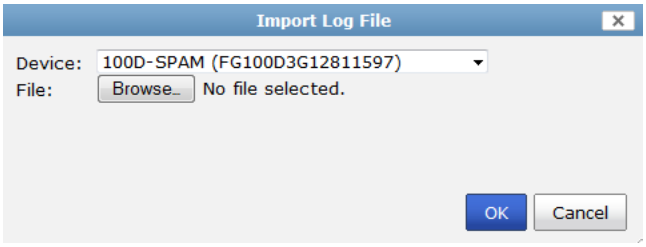
Imported log files can be useful when restoring data, or loading log data for temporary use. For example, if you have older log files from a device, you can import these logs to the FortiManager unit so that you can generate reports containing older data. Importing log files is also useful when changing your RAID configuration. Changing your RAID configuration reformats the hard disk, erasing log files. If you back up the log files, after changing the RAID configuration, you can import logs to restore them to the FortiManager unit.

To import a log file:

1. Go to *Log View* > *Log Browse*.
2. Select *Import* in the toolbar.

   The *Import Log File* dialog box opens.

   Figure 234: Import log file dialog box



3. Select the device to which the imported log file belongs from the *Device* field drop-down list, or select *[Take From Imported File]* to read the device ID from the log file.

   If you select *[Take From Imported File]* your log file must contain a `device_id` field in its log messages.
4. In the *File* field, enter the path and file name of the log file, or select *Browse*. and browse to the log file.

5. Select *OK*.

   A message appears, stating that the upload is beginning, but will be cancelled if you leave the page.

6. Select *OK*.

   The upload time varies depending on the size of the file and the speed of the connection.

After the log file successfully uploads, the FortiManager unit inspects the log file.

- If the `device_id` field in the uploaded log file does not match the device, the import will fail. Select *Return* to attempt another import.
- If you selected *[Take From Imported File]*, and the FortiManager unit's device list does not currently contain that device, a message appears after the upload. Select *OK* to import the log file and automatically add the device to the device list, or select *Cancel*.

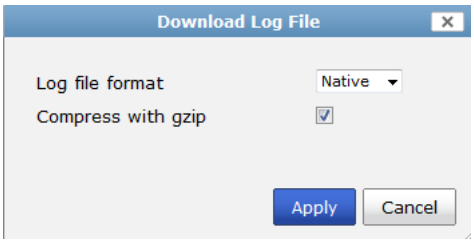
Downloading a log file

You can download a log file to save it as a backup or for use outside the FortiManager unit. The download consists of either the entire log file, or a partial log file, as selected by your current log view filter settings and, if downloading a raw file, the time span specified.

To download a log file:

1. Go to *Log View* > *Log Browse*.
2. Select the specific log file (wlog.log, elog.log, etc.) that you want to download.
3. Select *Download* in the toolbar.
4. The Download Log File dialog box opens.

Figure 235: Download log file dialog box



5. Select *OK*.

   If prompted by your web browser, select a location to where save the file, or open the file without saving.

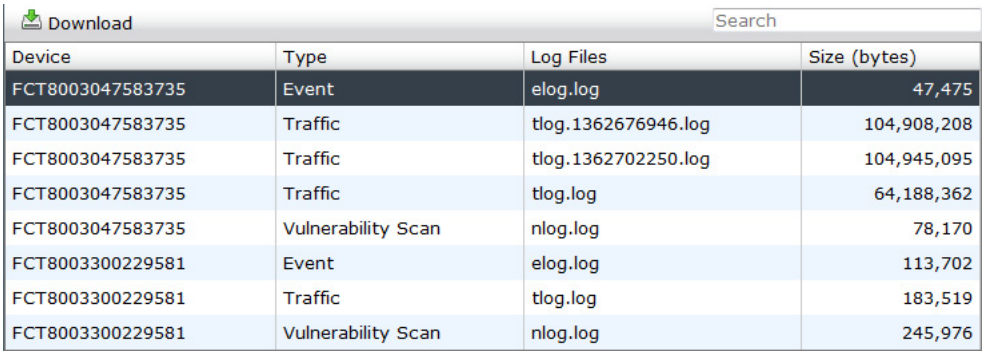
6. Select the log file format, either a text file, Native file, or a CSV file, and select *Compress with gzip* if you need to download a compressed file.
7. Select *OK*.

   If prompted by your web browser, select a location to where save the file, or open the file without saving.

FortiClient logs

The FortiManager can receive FortiClient logs uploaded through TCP port 514. The FortiClient logs can be viewed and downloaded from *Log View* > *FortiClient*.

Figure 236: FortiClient logs



Device	Type	Log Files	Size (bytes)
FCT8003047583735	Event	elog.log	47,475
FCT8003047583735	Traffic	tlog.1362676946.log	104,908,208
FCT8003047583735	Traffic	tlog.1362702250.log	104,945,095
FCT8003047583735	Traffic	tlog.log	64,188,362
FCT8003047583735	Vulnerability Scan	nlog.log	78,170
FCT8003300229581	Event	elog.log	113,702
FCT8003300229581	Traffic	tlog.log	183,519
FCT8003300229581	Vulnerability Scan	nlog.log	245,976

To download a FortiClient log file, select the desired log from the list, then select *Download* from the toolbar. In the confirmation dialog box, select if you want to compress the log file with gzip, then select *Apply* to download the log file.

For more information, see the *FortiClient v5.0 Patch Release 4 Administration Guide*.

Configuring rolling and uploading of logs

You can control device log file size and consumption of the FortiManager's disk space by configuring log rolling and scheduled uploads to a server.

As the FortiManager unit receives new log items, it performs the following tasks:

- verifies whether the log file has exceeded its file size limit
- checks to see if it is time to roll the log file if the file size is not exceeded.

Configure the time to be either a daily or weekly occurrence, and when the roll occurs. When a current log file (`tlog.log`) reaches its maximum size, or reaches the scheduled time, the FortiManager unit rolls the active log file by renaming the file. The file name will be in the form of `xlog.N.log` (for example, `tlog.1252929496.log`), where `x` is a letter indicating the log type and `N` is a unique number corresponding to the time the first log entry was received. The file modification time will match the time when the last log was received in the log file.

Once the current log file is rolled into a numbered log file, it will not be changed. New logs will be stored in the new current log called `tlog.log`. If log uploading is enabled, once logs are uploaded to the remote server or downloaded via the Web-based Manager, they are in the following format:

```
FG3K6A3406600001-tlog.1252929496.log-2012-09-29-08-03-54.gz
```

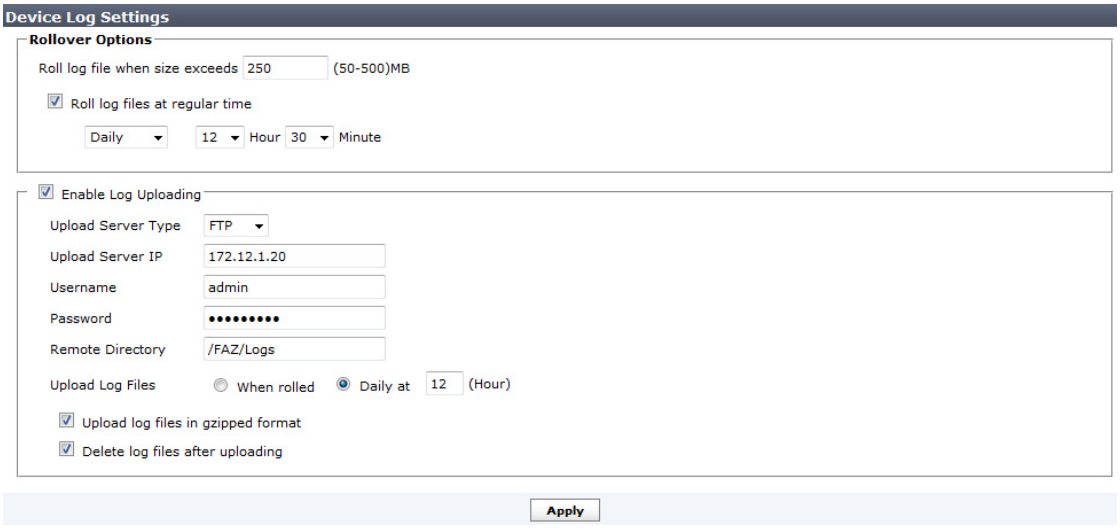
If you have enabled log uploading, you can choose to automatically delete the rolled log file after uploading, thereby freeing the amount of disk space used by rolled log files. If the log upload fails, such as when the FTP server is unavailable, the logs are uploaded during the next scheduled upload.

Log rolling and uploading can be enabled and configured in the Web-based Manager in *System Settings* > *Advanced* > *Device Log Settings*.

The device log settings menu window, found at *System Settings* > *Advanced* > *Device Log Settings*, allows you to configure event logging to disk and includes the following options:

- Log rollover options
- Log upload to an FTP, SFTP or SCP server

Figure 237: Device log settings window



Configure the following settings and then select *Apply*:

Rollover Options	
Roll log file when size exceeds	Enter the log file size. Enter a value between 50 to 500 MB.
Roll log files at a regular time	Select to roll logs daily or weekly. When selecting daily, select the hour and minute value in the drop-down lists. When selecting weekly, select the day, hour, and minute value in the drop-down lists.
Enable log uploading	Select to upload real time device logs.
Upload Server Type	Select one of *FTP, SFTP*, or *SCP*.
Upload Server IP	Enter the IP address of the upload server.
Username	Select the username that will be used to connect to the upload server.
Password	Select the password that will be used to connect to the upload server.
Remote Directory	Select the remote directory on the upload server where the log will be uploaded.
Upload Log Files	Select to upload log files when they are rolled according to settings selected under *Roll Logs* or daily at a specific hour.

Upload rolled files in gzipped format	Select to gzip the logs before uploading. This will result in smaller logs, and faster upload times.
Delete files after uploading	Select to remove device log files from the FortiManager system after they have been uploaded to the Upload Server.

Log rolling and uploading can also be enabled and configured using CLI commands. For more information, see the *FortiManager v5.0 Patch Release 5 CLI Reference*.

To enable or disable log file uploads:

To enable log uploads, enter the following CLI commands:

```
config system log settings
  config rolling-regular
    set upload enable
    set del-files {enable | disable}
    set directory <string>
    set file-size <integer>
    set gzip-format {enable | disable}
    set ip <server_ipv4>
    set log-format {csv | native | text}
    set password <string>
    set server_type {ftp | scp | sftp}
    set upload-hour <integer>
    set upload-trigger {on-roll | on-schedule}
    set username <string>
    set when {daily | none | weekly}
    end
  end
```

where:

`del-files {enable | disable}`	Delete the log files from the FortiManager hard disk one uploading is complete.
`directory <string>`	The directory on the upload server where the FortiManager unit stores the uploaded logs. The maximum length is 128 characters.
`file-size <integer>`	Roll log files when they reach this size (MB).
`gzip-format {enable | disable}`	Compress the log files using the gzip format.
`ip <server_ipv4>`	The upload server's IP address.
`log-format {csv | native | text}`	The format of the uploaded log files: • `csv`: CSV (comma-separated value) format • `native`: Native format (text or compact) • `text`: Text format (convert if necessary)
`server_type {ftp | scp | sftp}`	The type of upload server.

`upload-hour <integer>`	The hour that the log files are uploaded. The default is zero. Enter the number, without minutes, in the 24-hour format.
`upload-trigger {on-roll | on-schedule}`	The type of trigger will upload log files. • `on-roll` will upload log files whenever they roll. • `on-schedule` will upload log files on a scheduled basis.
`username <string>`	The upload server user name. The maximum length is 36 characters.
`password <string>`	The upload server password.
`when {daily | none | weekly}`	Select when to roll log files. Select daily, weekly, or none.

To disable log uploads, enter the following CLI commands:

```
config system log settings
  config rolling-regular
    set upload disable
    end
  end
```

To roll logs when they reach a specific size:

Enter the following CLI commands:

```
config system log settings
  config rolling-regular
    set file-size <integer>
    end
  end
```

where `<integer>` is the size at which the logs will roll, in MB.

To roll logs on a schedule:

To disable log rolling, enter the following CLI commands:

```
config system log settings
  config rolling-regular
    set when none
    end
  end
```

To enable daily log rolling, enter the following CLI commands:

```
config system log settings
  config rolling-regular
    set upload enble
    set when daily
    set hour <integer>
    set min <integer>
    set file-size <integer>
    end
  end
```

where:

`hour <integer>`	The hour of the day when the when the FortiManager rolls the traffic analyzer logs.
`min <integer>`	The minute when the FortiManager rolls the traffic analyzer logs.
`file-size <integer>`	Roll log files when they reach this size (MB).

To enable weekly log rolling, enter the following CLI commands:

```
config system log settings
  config rolling-regular
    set when weekly
    set days {mon | tue | wed | thu | fri | sat | sun}
    set hour <integer>
    set min <integer>
    end
  end
```

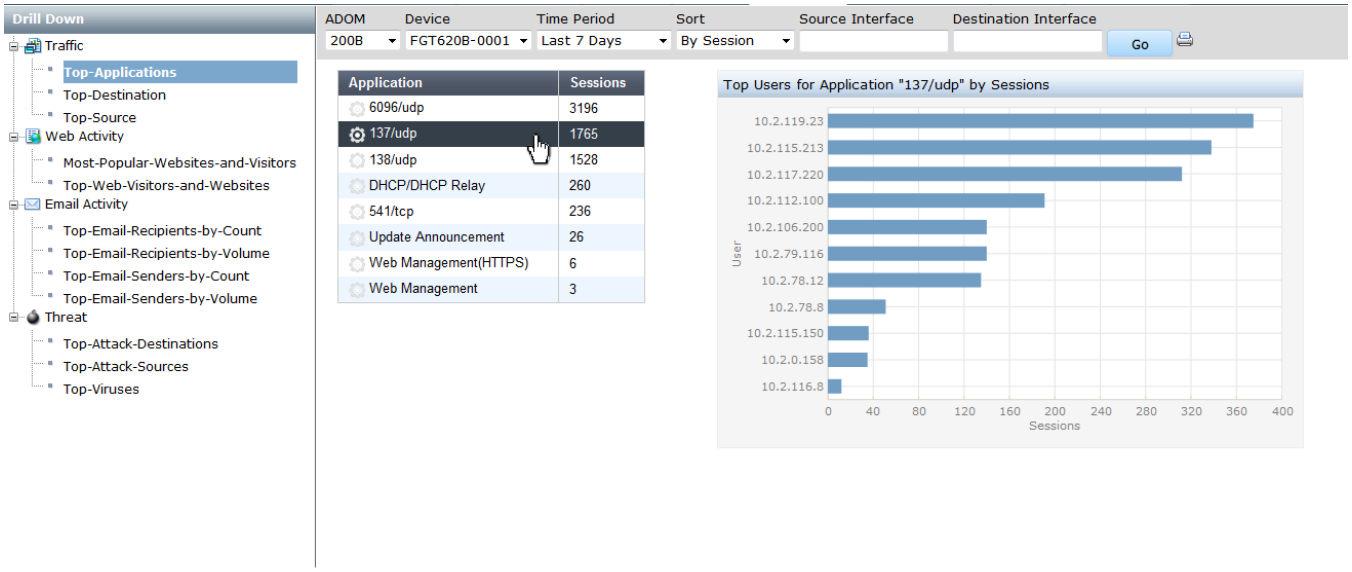
where:

`days {mon | tue | wed | thu | fri | sat | sun}`	The days week when the FortiManager rolls the traffic analyzer logs.
`hour <integer>`	The hour of the day when the when the FortiManager rolls the traffic analyzer logs.
`min <integer>`	The minute when the FortiManager rolls the traffic analyzer logs.

Drill Down

The *Drill Down* tab allows you to generate ad-hoc graphical views of traffic, web, email, and threat activity on an individual FortiGate device, VDOM, or log array. Similar to the log view feature, if a FortiGate device belongs to a log view group, it will no longer be available as an individual device.

Figure 238: Drill Down tab and data



Traffic activity

FortiManager has a fixed subset of drill downs for traffic activity. You can view and drill down top applications, top destinations, and top source data for an individual device, VDOM, or log array that is configured to log to your FortiManager device. This data can be populated for the last 30 minutes, 1 hour, 4 hours, 12 hours, 1 day or 7 days.

To display traffic drill down data:

1. Select either *Top-Applications*, *Top-Destination*, or *Top-Source* in the *Traffic* tree menu.
2. In the *ADOM* field, select an ADOM from the drop-down list.
3. In the *Device* field, select a device, VDOM, or log array from the drop-down list.
4. In the *Time Period* field, select the desired time period from the drop-down list.
5. In the *Sort* field, select either *By Session* or *By Bandwidth* from the drop-down list.
6. Optionally, you can enter a source interface and destination interface to filter data.
7. Select *Go* in the toolbar to populate data for the selected device, VDOM, or log array.

To drill down populated data:

1. In the table displayed, select one of the fields to display the drill down information. The drill down table is displayed.

2. Hover the mouse over the drill down chart to view detailed information for the entry. You can select the print icon in the toolbar to print the drill down data.

Web activity

FortiManager has a fixed subset of drill downs for web activity. You can drill down the most popular websites and visitors and top web visitors and websites for an individual device, VDOM, or log array that is configured to log to your FortiManager device. This data can be populated for the last 30 minutes, 1 hour, 4 hours, 12 hours, 1 day or 7 days.

To display web activity drill down data:

1. Select either *Most-Popular-Websites-and-Visitors* or *Top-Web-Visitors-and-Websites* in the *Web Activity* tree menu.
2. In the *ADOM* field, select an ADOM from the drop-down list.
3. In the *Device* field, select a device, VDOM, or log array from the drop-down list.
4. In the *Time Period* field, select the desired time period from the drop-down list.
5. Select *Go* in the toolbar to populate data for the selected device, VDOM, or log array.

To drill down populated data:

1. In the table displayed, select one of the fields to display the drill down information. The drill down table is displayed.
2. Hover the mouse over the drill down chart to view detailed information for the entry. You can select the print icon in the toolbar to print the drill down data.

Email activity

FortiManager has a fixed subset of drill downs for email activity. You can drill down top email recipients and top email senders by count or by volume for an individual device, VDOM, or log array that is configured to log to your FortiManager device. This data can be populated for the last 30 minutes, 1 hour, 4 hours, 12 hours, 1 day or 7 days.

To display web activity drill down data:

1. Select either *Top-Email-Recipients-by-Count*, *Top-Email-Recipients- by-Volume*, *Top-Email-Senders-by-Count*, or *Top-Email-Senders-by-Volume* in the *Email Activity* tree menu.
2. In the *ADOM* field, select an ADOM from the drop-down list.
3. In the *Device* field, select a device, VDOM, or log array from the drop-down list.
4. In the *Time Period* field, select the desired time period from the drop-down list.
5. Select *Go* in the toolbar to populate data for the selected device, VDOM, or log array.

To drill down populated data:

1. In the table displayed, select one of the fields to display the drill down information. The drill down table is displayed.
2. You can select the print icon in the toolbar to print the drill down data.

Threat activity

FortiManager has a fixed subset of drill downs for threat activity. You can drill down top attack destinations, top attack sources, and top viruses for an individual device, VDOM, or log array that is configured to log to your FortiManager device. This data can be populated for the last 30 minutes, 1 hour, 4 hours, 12 hours, 1 day or 7 days.

To display web activity drill down data:

1. Select either *Top-Attack-Destinations*, *Top-Attack-Sources*, or *Top-Viruses* in the *Threat* tree menu.
2. In the *ADOM* field, select an ADOM from the drop-down list.
3. In the *Device* field, select a device, VDOM, or log array from the drop-down list.
4. In the *Time Period* field, select the desired time period from the drop-down list.
5. Select *Go* in the toolbar to populate data for the selected device, VDOM, or log array.

To drill down populated data:

1. In the table displayed, select one of the fields to display the drill down information. The drill down table is displayed.
2. You can select the print icon in the toolbar to print the drill down data.

Event Management

In Event Management you can configure events handlers based on log type and logging filters. You can select to send the event to an email address, SNMP community, or syslog server. Events can be configured per device, per log array, or for all devices. You can create event handlers for FortiGate, FortiCarrier, FortiMail, and FortiWeb devices.

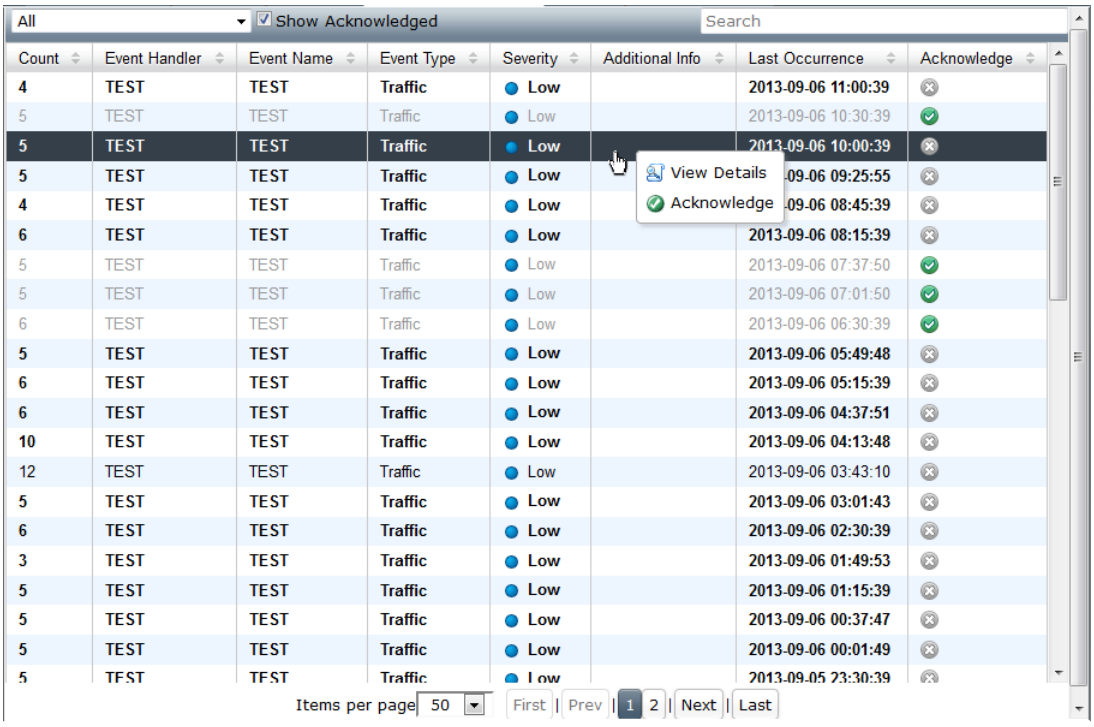
Events

Events can also be monitored and the logs associated with a given event can be viewed.

The events page provides a list of the generated events. Right-clicking on an event in the table gives you the option of viewing event details including the raw log entries associated with that event, adding review notes, and acknowledging the event.

To view events, go to the *Event Management* tab and select *Event Management* > *All Events.* You can also view events by severity and by handler. When ADOMs are enabled, select the ADOM, and then select *All Events*. FortiMail and FortiWeb events are listed in their respective default ADOM.

Figure 239: Events page



The following table lists page information and options:

Time Period	Select a time period from the drop-down list. Select one of: *All*, *Last 1 hour*, *Last 1 day*, *Last 7 days*, or *Last 30 days*.
Show/Hide Acknowledged	Select to show or hide acknowledged events. Acknowledged events are greyed out in the list.
Search	Search for a specific event.
Count	The number of log entries associated with the event. Click the heading to sort events by count.
Event Handler	The name of the *Event Handler* that triggered the event. Click the heading to sort events by event handler.
Event Name	The name of the event. Click the heading to sort events by event name.
Event Type	The event type. For example, *Traffic* or *Event.* Click the heading to sort events by event type.
Severity	The severity level of the event. Event severity level is a user configured variable. The severity can be *Critical, High, Medium,* or *Low*. Click the heading to sort events by severity.
Additional Info	Additional information about the event. Click the heading to sort events by additional information.
Last Occurrence	The date and time that the event was created and added to the events page. Click the heading to sort events by last occurrence.
Acknowledge	Displays a grey circle icon with an “x” when the event has not been acknowledged and a green circle icon with a check mark when the event has been acknowledged. Click the heading to sort events by last acknowledged status.
Items per page	Select to display 50, 100, or 150 items per page.
First, Prev, 1, 2, .., Next Last	Navigate pages in the events page.
View Details	Select an event entry, right-click, and select *View Details* in the menu. The *Event Details* page will be displayed.
Acknowledge	Select an event entry, right-click, and select *Acknowledge* in the menu to remove the event from the list.

Event details

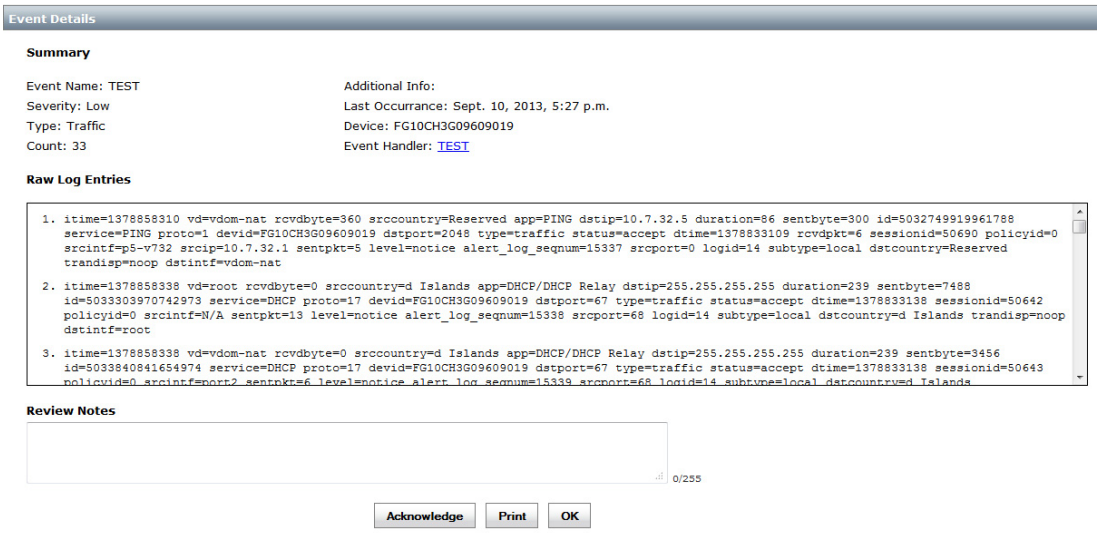
Event details provides a summary of the event including the event name, severity, type, count, additional information, last occurrence, device, event handler, raw log entries, and review notes. You can also acknowledge and print events in this page.

To view log messages associated with an event:

1. Go to *Event Management* > *All Events*.
2. Select the event, right-click, and select *View Details* in the menu.

   The *Event Details* page is displayed.

Figure 240: Event details page



3. In this page you can view raw log entries, enter review notes, acknowledge the event, or print the event details. You can also click the event handler link to view the event handler that triggered the event.
4. Select *OK* to return to the *All Events* page.

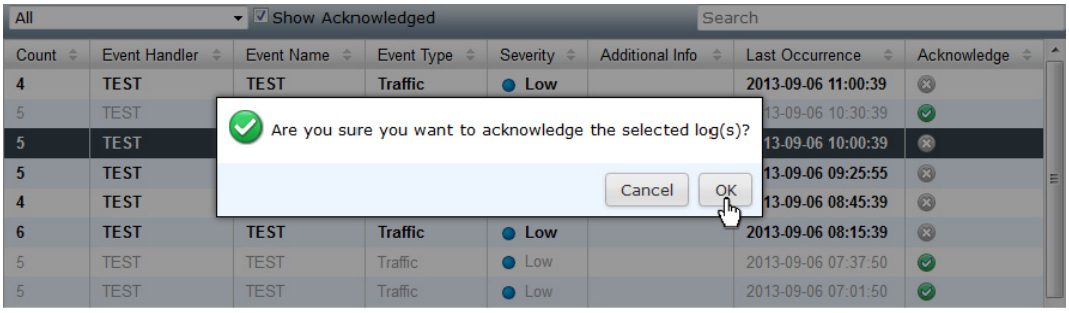
Acknowledge events

You can select to acknowledge events to remove them from the event list. An option has been added to this page to allow you to show or hide these acknowledged events.

To acknowledge events:

1. Go to *Event Management* > *All Events* and select the event or events you would like to acknowledge. To select multiple alert events press the CTRL button and select events using the left-click button on your mouse.
2. Right-click and select *Acknowledge* in the menu.
3. Select *OK* in the confirmation dialog box to acknowledge the selected alert event or events.

Figure 241: Confirmation dialog box



Select the *Show Acknowledge* checkbox in the toolbar to view acknowledged events.

Event handler

Event handler allows you to view, create new, edit, delete, clone, and search event handlers. You can select these options in the toolbar. The right-click menu includes these options and also includes the ability to enable or disable configured event handlers. You can create event handlers for a specific device, multiple devices, or log arrays. You can select to create event handlers for traffic logs or event logs. Events for FortiMail and FortiWeb devices are created within their respective ADOMs.

FortiManager v5.0 Patch Release 5 includes five default event handlers for FortiGate and FortiCarrier devices. Click on the event handler name to enable or disable the event handler and to assign devices to the event handler. The default event handlers are disabled by default.

Table 14: Default event handlers

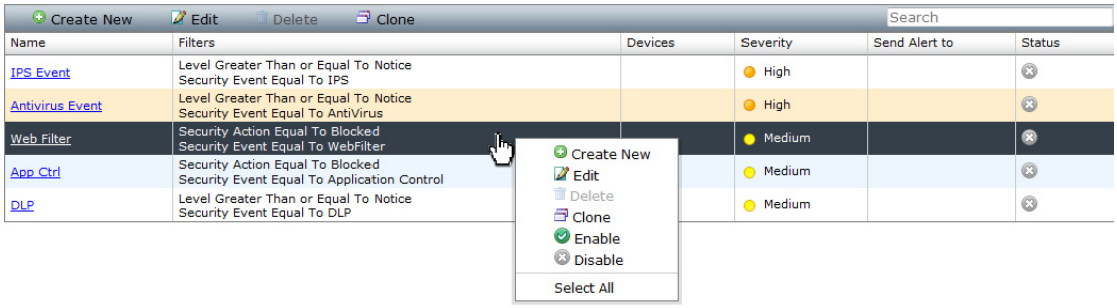
Event Handler	Description
Antivirus Event	Severity: High Filters: Traffic Log, Log messages that match all conditions: • *Level Greater Than or Equal To Notice* • *Security Event Equal To AntiVirus* Event Handling: Generate alert when 1 or more of each type occur in 30 minutes
APP Ctrl	Severity: Medium Filters: Traffic Log, Log messages that match all conditions: • *Security Action Equal To Blocked* • *Security Event Equal To Application Control* Event Handling: Generate alert when 1 or more of each type occur in 30 minutes
DLP	Severity: Medium Filters: Traffic Log, Log messages that match all conditions: • *Level Greater Than or Equal To Notice* • *Security Event Equal To DLP* Event Handling: Generate alert when 1 or more of each type occur in 30 minutes

Table 14: Default event handlers (continued)

Event Handler	Description
Antivirus Event	Severity: High Filters: Traffic Log, Log messages that match all conditions: • *Level Greater Than or Equal To Notice* • *Security Event Equal To AntiVirus* Event Handling: Generate alert when 1 or more of each type occur in 30 minutes
IPS Event	Severity: High Filters: Traffic Log, Log messages that match all conditions: • *Level Greater Than or Equal To Notice* • *Security Event Equal To IPS* Event Handling: Generate alert when 1 or more of each type occur in 30 minutes
Web Filter	Severity: Medium Filters: Traffic Log, Log messages that match all conditions: • *Security Action Equal to Blocked* • *Security Event Equal to WebFilter* Event Handling: Generate alert when 1 or more of each type occur in 30 minutes

Go to the *Event Management* tab and select *Event Handler* in the tree menu.

Figure 242: Event handler page



The following table lists page information and options:

Name	The name of the event handler.
Filters	The filters that you have configured for the event handler.
Devices	The devices that you have configured for the event handler. This field will either display *All FortiGates* or list each device or log array.
Severity	The severity that you configured for the event handler. This field will display *Critical, High, Medium*, or *Low*.

Send Alert to	The email address, SNMP server, or syslog server that has been configured for the event handler.
Status	The status of the event handler. This field will display a green circle check mark when enabled or a grey circle x when disabled.
Create New	Select to create a new event handler. This option is available in the toolbar and right-click menu.
Edit	Select an event handler and select edit to make changes to the entry. This option is available in the toolbar and right-click menu.
Delete	Select one or all event handlers and select delete to remove the entry(s). This option is available in the toolbar and right-click menu. The default event handlers cannot be deleted.
Clone	Select an event handler in this page and click to clone the entry. A cloned entry will have Copy added to the name field. You can rename the cloned entry while editing the event handler. This option is available in the toolbar and right-click menu.
Select All	Select an event handler and select *Select All* in the right-click pop-up menu. You can then select *Delete* in the toolbar to select all entries.
Enable	Select an event handler and select *Enable* in the right-click pop-up menu.
Disable	Select an event handler and select *Disable* in the right-click pop-up menu.

Traffic log events

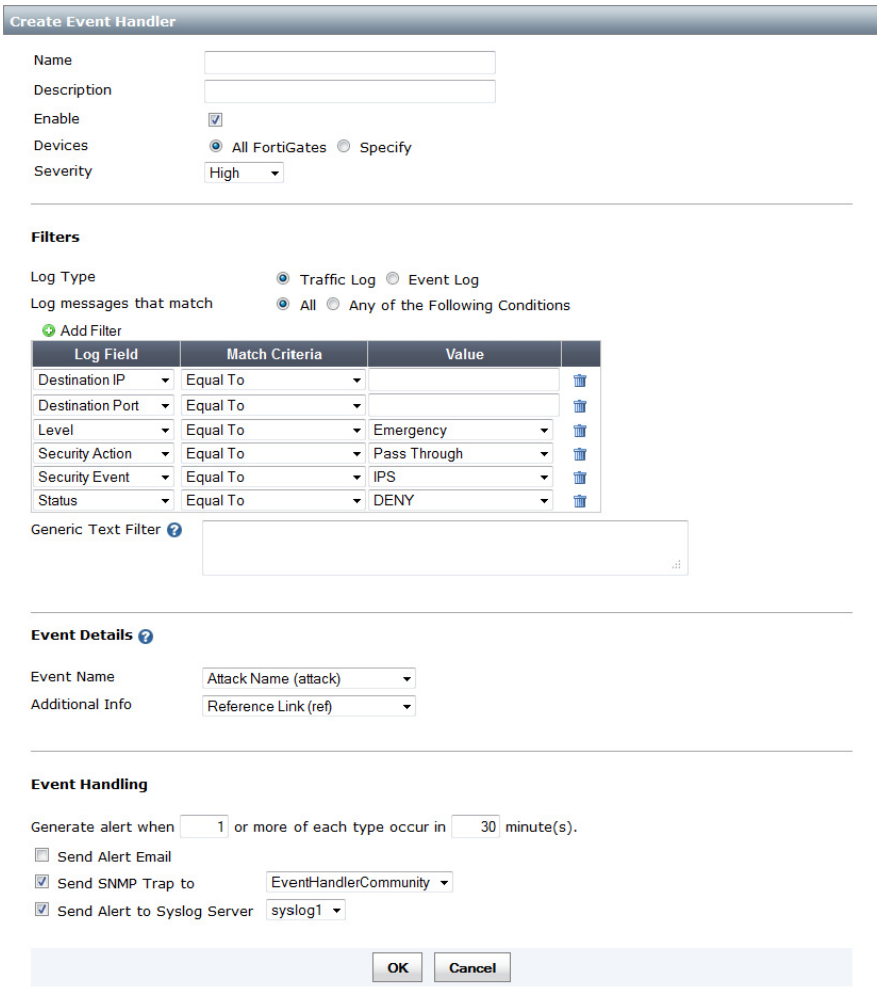
You can create traffic log event handlers to monitor network traffic based on specific log filters.

Create a new event handler (traffic log):

1. Go to *Event Management* > *Event Handler*.
2. Select *Create New* in the toolbar. Optionally, you can right-click the entry and select *Create New* in the pop-up menu.

   The *Create Event Handler* page opens.

Figure 243: Create event handler page



3. Configure the following settings:

Name	Enter a name for the event handler.
Description	Enter a description for the event handler.
Enable	Select to enable the event handler.

Devices	Select *All FortiGates* or select *Specify* and use the plus (+) symbol to add devices or log arrays. Note: When creating a new event handler for FortiMail and FortiWeb, the *All FortiGates* option is a bug.
Severity	Select the severity from the drop-down list. Select one of the following: *Critical, High, Medium*, or *Low*.
Filters	
Log Type	Select *Traffic Log*.
Log message that match	Select either *All* or *Any of the Following Conditions*.
Add Filter	Select the plus (+) symbol to add log filters.
Destination IP	Select *Destination IP* from the *Log Field* drop-down list. Select either *Equal To* or *Not Equal To* in the *Match Criteria* drop-down list. Enter a destination IP in the *Value* text field. Select the garbage can icon to delete the filter.
Destination Port	Select *Destination Port* from the *Log Field* drop-down list. Select one of *Equal To, Not Equal To, Greater Than or Equal To, Less Than or Equal To, Greater Than,* or *Less Than* in the *Match Criteria* drop-down list. Enter a destination port in the *Value* text field. Select the garbage can icon to delete the filter.
Level	Select *Level* from the *Log Field* drop-down list. Select one of *Equal To, Not Equal To, Greater Than or Equal To, Less Than or Equal To, Greater Than,* or *Less Than* in the *Match Criteria* drop-down list. Select the logging level (Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug) from the *Value* drop-down list. Select the garbage can icon to delete the filter.
Security Event	Select *Security Event* from the *Log Field* drop-down list. Select either *Equal To* in the *Match Criteria* drop-down list. Select either *AntiVirus*, *WebFilter*, *Application Control, DLP*, or *IPS* from the *Value* drop-down list. Select the garbage can icon to delete the filter.
Status	Select *Status* from the *Log Field* drop-down list. Select either *Equal To* or *Not Equal To* in the *Match Criteria* drop-down list. Select either *DENY*, *ACCEPT*, *START*, *DNS*, *IP-CONN*, *WEB*, *CLOSE*, or *TIMEOUT* from the *Value* drop-down list. Select the garbage can icon to delete the filter.
Generic Text Filter	Enter a generic text filter. For more information on creating a text filter select the help icon.
Event Details	Only available when you have one *Security Event* filter or the *Log Type* is *Event Log*.
Event Name	Select an event name from the drop-down list. The options in the list are dependent on the specific security event selected.

Additional Info	Select additional information from the drop-down list. The options in the list are dependent on the specific security event selected.
Event Handling	
Generate alerts when ...	Enter threshold values to generate alerts and 'x' or more of each type occur in 'x' minutes.
Send Alert Email	Select the checkbox to enable. Enter an email address in the *To* and *From* text fields and select the email server from the drop-down list. To create a new mail server, select the *System Settings* tab, select *Advanced* > *Mail Server*, and select *Create New* in the toolbar.
Send SNMP Trap to	Select the checkbox to enable this feature. Select an SNMP community from the drop-down list. To create a new SNMP community, select the *System Settings* tab, select *Advanced* > *SNMP v1/v2*, select the checkbox to enable the SNMP agent. In the *Communities* section, select *Create New* in the toolbar.
Send Alert to Syslog Server	Select the checkbox to enable this feature. Select a syslog server from the drop-down list. To create a syslog server, select the *System Settings* tab, select *Advanced* > *Syslog Server*, and select *Create New* in the toolbar.

4. Select *OK* to save the configuration.

Event log alerts

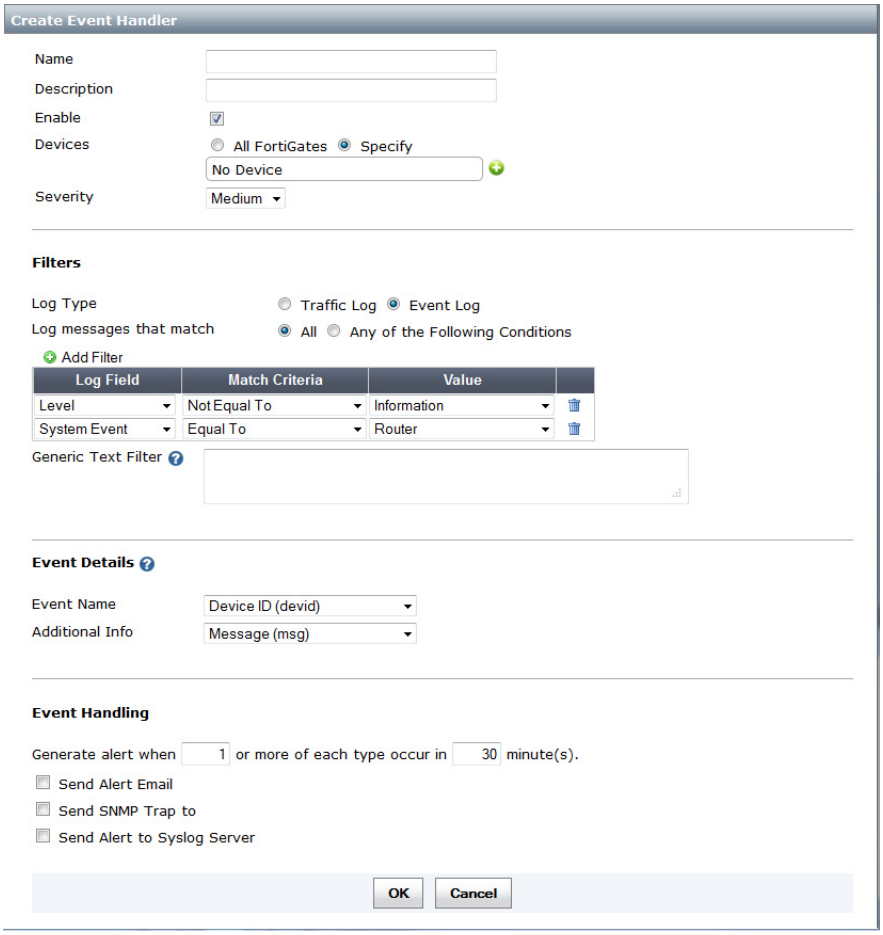
You can create event log event handlers to monitor network events based on specific log filters.

Create a new event handler (event log):

1. Go to *Event Management* > *Event Handler*.
2. Select *Create New* in the toolbar. Optionally, you can right-click the entry and select *Create New* in the pop-up menu.

   The *Create Event Handler* page opens.

Figure 244: Create event handler page



3. Configure the following settings:

Name	Enter a name for the event handler.
Description	Enter a description for the event handler.
Enable	Select to enable the event handler.
Devices	Select *All FortiGates* or select *Specify* and use the plus (+) symbol to add devices or log arrays. Note: When creating a new event handler for FortiMail and FortiWeb, the *All FortiGates* option is a bug.
Severity	Select the severity from the drop-down list. Select one of the following: *Critical, High, Medium*, or *Low*.
Filters	
Log Type	Select *Event Log*.
Log message that match	Select either *All* or *Any of the Following Conditions*.
Add Filter	Select the plus (+) symbol to add log filters.

Level	Select *Level* from the *Log Field* drop-down list. Select either *Equal To, Not Equal To, Greater Than or Equal To, Less Than or Equal To, Greater Than,* or *Less Than* in the *Match Criteria* drop-down list. Select the logging level (Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug) from the *Value* drop-down list. Select the garbage can icon to delete the filter.
System Event	Select *System Event* from the *Log Field* drop-down list. Select either *Equal To* or *Not Equal To* in the *Match Criteria* drop-down list. Select either *System*, *Router*, *VPN*, *User*, *WAN Optimization* or *Wireless* from the *Value* drop-down list. Select the garbage can icon to delete the filter.
Generic Text Filter	Enter a generic text filter. For more information on creating a text filter select the help icon.
Event Details	Only available when you have one *Security Event* filter or the *Log Type* is *Event Log*.
Event Name	Select an event name from the drop-down list. The options in the list are dependent on the specific security event selected.
Additional Info	Select additional information from the drop-down list. The options in the list are dependent on the specific security event selected.
Event Handling	
Generate alerts when ...	Enter threshold values to generate alerts and 'x' or more of each type occur in 'x' minutes.
Send Alert Email	Select the checkbox to enable. Enter an email address in the *To* and *From* text fields and select the email server from the drop-down list. To create a new mail server, select the *System Settings* tab, select *Advanced* > *Mail Server*, and select *Create New* in the toolbar.
Send SNMP Trap to	Select the checkbox to enable this feature. Select an SNMP community from the drop-down list. To create a new SNMP community, select the *System Settings* tab, select *Advanced* > *SNMP v1/v2*, select the checkbox to enable the SNMP agent. In the *Communities* section, select *Create New* in the toolbar.
Send Alert to Syslog Server	Select the checkbox to enable this feature. Select a syslog server from the drop-down list. To create a syslog server, select the *System Settings* tab, select *Advanced* > *Syslog Server*, and select *Create New* in the toolbar.

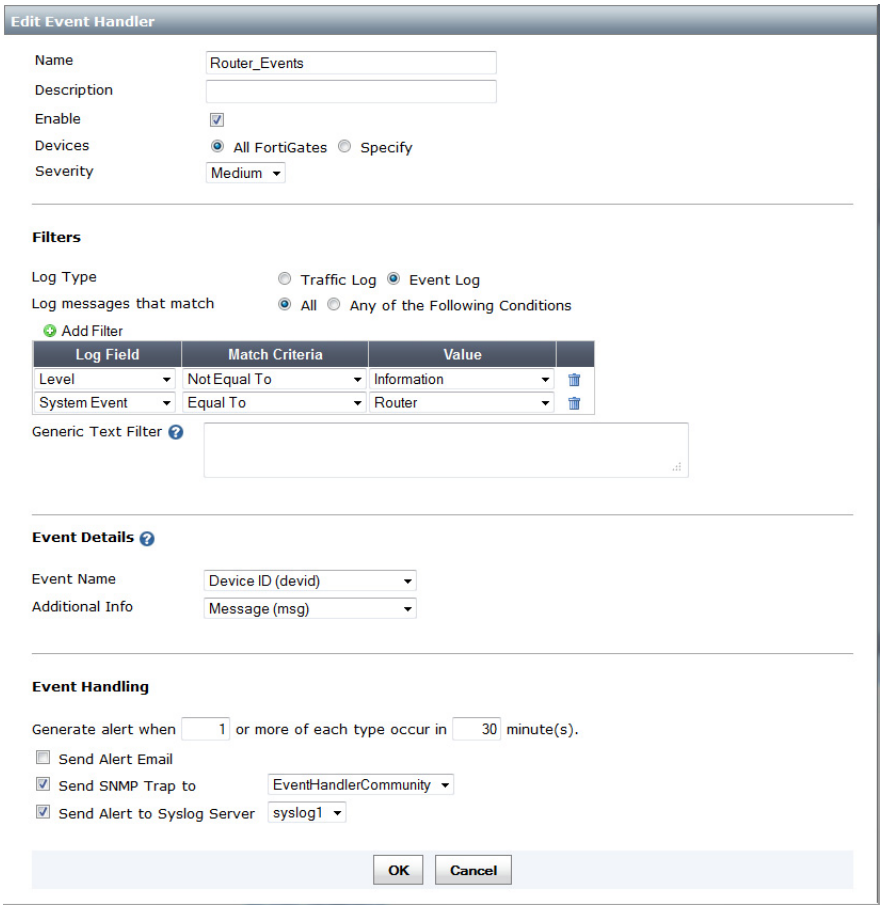
Select *OK* to save the configuration.

To edit an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry and select *Edit* in the toolbar. Optionally, you can right-click the entry and select *Edit* in the pop-up menu.

   The *Edit Event Handler* page opens.

Figure 245: Edit event handler page



3. Edit the settings as required.
4. Select *OK* to save the configuration.

To clone an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry and select *Clone* in the toolbar. Optionally, you can right-click the entry and select *Clone* in the pop-up menu. The *Clone Event Handler* window opens.
3. Edit the settings as required.
4. Select *OK* to save the configuration.

To delete an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry and select *Delete* in the toolbar. Optionally, you can right-click the entry and select *Delete* in the pop-up menu.
3. Select *OK* in the confirmation dialog box to proceed.



Select *Select All* in the right-click menu to select all alert event entries. You can then select *Delete* in the toolbar to delete the selected entries.



The default event handlers cannot be deleted. Use the right-click menu to enable or disable these event handlers.

To enable an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry, right-click and select *Enable* in the pop-up menu. The status field will display a green circle check mark icon.

To disable an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry, right-click and select *Disable* in the pop-up menu. The status field will display a grey circle x icon.

Reports

FortiManager units can analyze information collected from the log files of managed log devices. It then presents the information in tabular and graphical reports. These reports provide a quick and detailed analysis of activity on your networks.

To reduce the number of reports needed, reports are independent from devices, and contain layout information in the form of a report template. The devices and any other required data related information can be added as parameters to the report at the time of report generation.



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

The *Reports* tab allows you to configure reports using the predefined report templates, configure report schedules, view report history and the report calendar, and configure and view charts, datasets, and output profiles.

This chapter contains the following sections:

- Report templates
- Schedules
- Reports
- Chart library
- Report calendar
- Advanced chart option



If ADOMs are enabled, each ADOM will have its own report settings.



FortiMail and FortiWeb reports are available when ADOMs are enabled. Reports for these devices are configured within their respective default ADOM. FortiMail and FortiWeb have device specific charts and datasets.

Report templates

The FortiManager has 13 preconfigured reports and report templates for FortiGate log devices. FortiMail and FortiWeb log devices have one default report. These report templates can be used as is, and you can also clone or edit the template. You can also create new reports and report templates and customize them as required. The following table lists the report templates and charts.

Table 15: Report templates

Report Template	Charts
FortiGate	
Admin and System Events Report	• Admin-Login-System-Events • System-Active-Summary
Application and Risk Analysis	Security Report • App-Risk-Top-Users-By-Bandwidth • App-Risk-Top-User-Source-By-Sessions • App-Risk-Top-Users-By-Reputation-Scores-Bar • App-Risk-Top-Devices-By-Reputation-Scores • App-Risk-Application-Usage-By-Category-With-Pie • App-Risk-App-Usage-By-Category • App-Risk-Breakdown-Of-Risk-Applications • App-Risk-Number-Of-Applications-By-Risk-Behavior • App-Risk-High-Risk-Application • App-Risk-Key-Applications-Crossing-The-Network • App-Risk-Applications-Running-Over-HTTP • App-Risk-Top-Web-Sites-Visited-By-Network-Users-Pie-Cha • App-Risk-Top-Web-Sites-Visited-By-Network-Users • App-Risk-Web-Browsing-Hostname-Category • Top-Destination-Countries-By-Browsing-Time • App-Risk-Traffic-Hostnames-By-Browsing-Time • App-Risk-Top-Threat-Vectors-Crossing-The-Network • App-Risk-Top-Critical-Threat-Vectors-Crossing-The-Network • App-Risk-Top-High-Threat-Vectors-Crossing-The-Network • App-Risk-Top-Medium-Threat-Vectors-Crossing-The-Network • App-Risk-Top-Low-Threat-Vectors-Crossing-The-Network • App-Risk-Top-Info-Threat-Vectors-Crossing-The-Network • App-Risk-Top-Virus-By-Name • App-Risk-Top-Virus-Victim • App-Risk-Malware-Discovered • App-Risk-Vulnerability-Discovered • App-Risk-Data-Los-Prevention-Type-Events

Table 15: Report templates (continued)

Report Template	Charts
Bandwidth and Applications Report	• Traffic-Bandwidth-Summary-Day-Of-Month • Session-Summary-Day-Of-Month • Top-Users-By-Bandwidth • Top-User-Source-By-Sessions • Top-App-By-Bandwidth • Top-App-By-Sessions • Top-Destination-Addresses-By-Bandwidth • Top-Destination-Addresses-By-Sessions • Top-Wifi-Clients-By-Bandwidth • Traffic-History-By-Active-User
Client Reputation	• Score-Summary-For-All-Users-Devices • Number-Of-Incidents-For-All-Users-Devices • Top-Users-By-Reputation-Scores • Top-Devices-By-Reputation-Scores • Top-Users-With-Increased-Scores • Top-Devices-With-Increased-Scores
Email Report	• Top-Email-Senders-By-Count • Top-Email-Senders-By-Bandwidth • Top-Email-Receivers-By-Count • Top-Email-Receivers-By-Bandwidth

Table 15: Report templates (continued)

Report Template	Charts
Security Analysis	Bandwidth and Applications • Traffic-Bandwidth-Summary-Day-Of-Month • Session-Summary-Day-Of-Month • Top-Users-By-Bandwidth • Top-User-Source-By-Sessions • Top-App-By-Bandwidth • Top-App-By-Sessions • Top-Destination-Addresses-By-Bandwidth • Top-Destination-Addresses-By-Bandwidth • DHCP-Summary-By-Port • Top-Wifi-Client-By-Bandwidth • Traffic-History-By-Active-User Web Usage • webfilter-Top-Web-Users-By-Blocked-Requests • webfilter-Top-Web-Users-By-Allowed-Requests • webfilter-Top-Users-By-Bandwidth • webfilter-Top-Web-Users-By-Browsing-Time • webfilter-Top-Blocked-Web-Sites-By-Requests • webfilter-Top-Allowed-Web-Sites-By-Requests • webfilter-Top-Allowed-Web-Sites-By-Bandwidth • traffic-Top-Domains-By-Browsing-Time Emails • Top-Email-Senders-By-Count • Top-Email-Senders-By-Bandwidth • Top-Email-Receivers-By-Count • Top-Email-Receivers-By-Bandwidth Threats • Top-Virus-By-Name • Top-Virus-Victim • Top-Attack-Source • Top-Attack-Victim VPN Usage • Top-Static-IPSEC-Tunnels-By-Bandwidth • Top-Dial-Up-IPSEC-Tunnels-By-Bandwidth • Top-SSL-VPN-Users-By-Bandwidth • Top-SSL-VPN-Web-Mode-Users-By-Bandwidth • vpn-Top-Dial-Up-VPN-Users-By-Duration • vpn-Traffic-Usage-Trend-VPN Admin and System Events • Admin-Login-System-Events • System-Active-Summary User Activity Summary • Top5-Users-By-Bandwidth

Table 15: Report templates (continued)

Report Template	Charts
Threat Report	Attacks • Top-Attack-Victim • Top-Attack-Source • Attacks-By-Severity • Intrusion-in-Last-7-Days • Top-Attacks-Detected • Top-Attacks-Blocked Virus • Top-Virus-Victim • Top-Virus-By-Name • Top-Virus-Source • Virus-Time-Line Web Filter • webfilter-Top-Web-Users-By-Blocked-Requests • webfilter-Top-Web-Users-By-Allowed-Requests • webfilter-Top-Blocked-Web-Sites-By-Requests • webfilter-Top-Allowed-Web-Sites-By-Requests • webfilter-Top-Blocked-Web-Categories • webfilter-Top-Allowed-Web-Categories • webfilter-Web-Activity-Summary-By-Requests Spyware • Top-Spyware-Victims • Top-Spyware-by-Name • Top-Spyware-Source • Spyware-Time-Line Adware • Top-Adware-Victims • Top-Adware-by-Name • Top-Adware-Source • Adware-Time-Line
User report	• Top5-Users-By-Bandwidth
User Security Analysis	• user-drilldown-Top-Blocked-Web-Sites-By-Requests • user-drilldown-Top-Allowed-Web-Sites-By-Requests • user-drilldown-Top-Blocked-Web-Categories • user-drilldown-Top-Allowed-Web-Categories • user-drilldown-Top-Attacks • user-drilldown-Top-Attacks-High Severity • user-drilldown-Top-Virus-By-Name • user-drilldown-Top-Virus-Receivers-Over-Email • user-drilldown-Count-Spam-Activity-by-Hour-of-Day • user-drilldown-Top-Spam-Sources

Table 15: Report templates (continued)

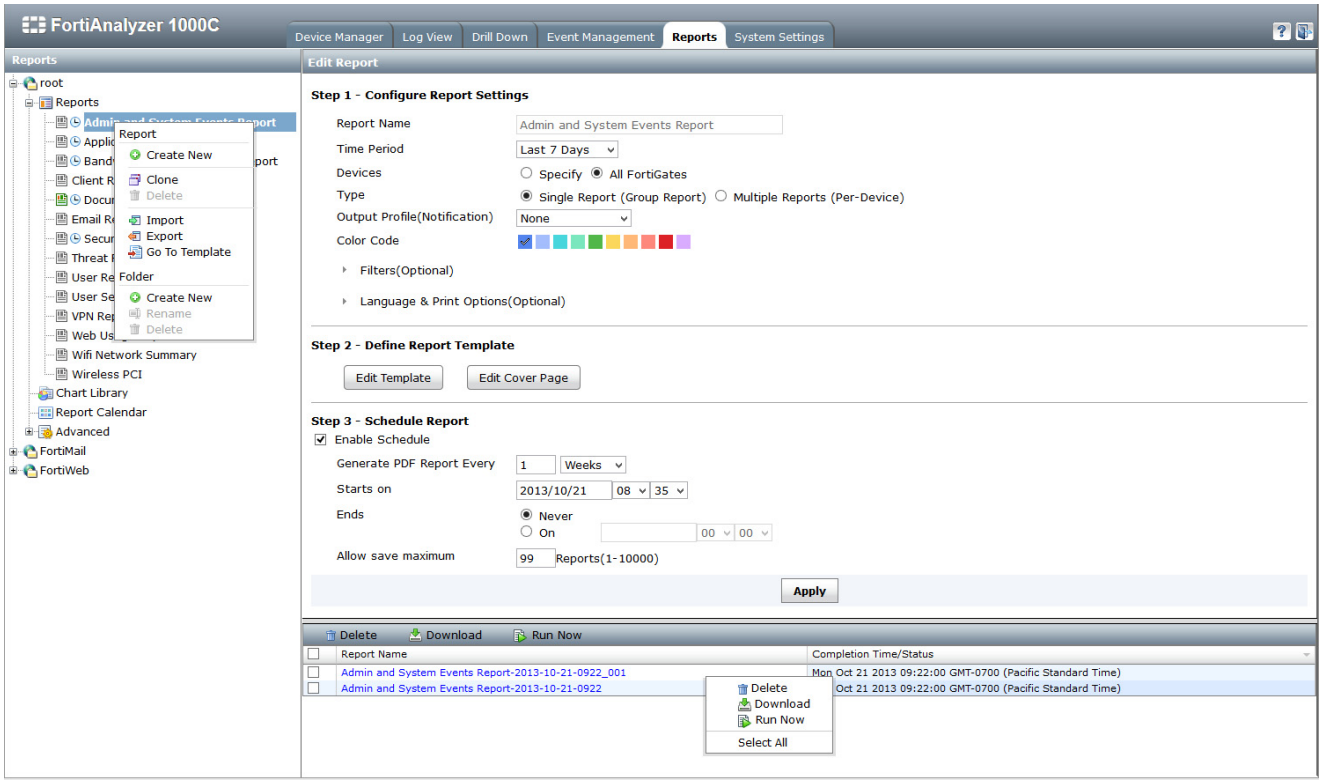
Report Template	Charts
VPN report	VPN Usage • vpn-Traffic-Usage-Trend-VPN • vpn-Top-Dial-Up-VPN-Users-By-Duration SSL VPN • default-Top-Sources-Of-SSL-VPN-Tunnels-By-Bandwidth • Top-SSL-VPN-Users-By-Bandwidth • Top-SSL-VPN-Web-Mode-Users-By-Bandwidth IPsec VPN • default-Top-Dial-Up-User-Of-Vpn-Tunnel-By-Bandwidth • Top-Static-IPSEC-Tunnels-By-Bandwidth • Top-Dial-Up-IPSEC-Tunnels-By-Bandwidth
Web Usage report	• webfilter-Web-Activity-Summary-By-Requests • traffic-Browsing-Time-Summary • webfilter-Top-Web-Users-By-Blocked-Requests • webfilter-Top-Web-Users-By-Allowed-Requests • webfilter-Top-Users-By-Bandwidth • traffic-Top-Web-Users-By-Browsing-Time • webfilter-Top-Blocked-Web-Sites-By-Requests • webfilter-Top-Allowed-Web-Sites-By-Requests • webfilter-Top-Allowed-Web-Sites-By-Bandwidth • webfilter-Top-Video-Streaming-Websites-By-Bandwidth • webfilter-Top-Blocked-Web-Categories • webfilter-Top-Allowed-Web-Categories • traffic-Top-Domains-By-Browsing-Time • traffic-Top-Destination-Countries-By-Browsing-Time • webfilter-Top-Search-Phrases
Wifi Network Summary	Network Summary • wifi-Overall-Traffic • wifi-Num-Distinct-Client Wireless Usage and Clients • wifi-Top-AP-By-Bandwidth • wifi-Top-AP-By-Client • wifi-Top-SSID-Bandwidth • wifi-Top-SSID-By-Client • wifi-Top-App-By-Bandwidth • wifi-Top-Client-By-Bandwidth • wifi-Top-OS-By-Bandwidth • wifi-Top-OS-By-Client • wifi-Top-Device-By-Bandwidth • wifi-Top-Device-By-Client

Table 15: Report templates (continued)

Report Template	Charts
Wireless PCI	• default-AP-Detection-Summary-by-Status-OnWire • default-AP-Detection-Summary-by-Status-OffWire • default-AP-Detection-Summary-by-Status-OnWire_table • default-AP-Detection-Summary-by-Status-OffWire_table • default-Managed-AP-Summary • default-Managed-AP-Summary_table • default-selected-AP-Details-OnWire • default-selected-AP-Details-OffWire • event-Wireless-Client-Details
FortiMail	
FortiMail Default Report	• fml-History-Top10-Client-IP • fml-History-Top10-Local-User • fml-History-Top10-Sender • fml-History-Top10-Recipient • fml-History-Top10-Virus-Sender • fml-History-Top10-Virus-Recipient
FortiWeb	
FortiWeb Default Report	• fwb-attack-Top-Attack-Sources • fwb-attack-Top-Attacked-Destinations • fwb-traffic-Top-Sources • fwb-traffic-Top-Destinations • fwb-event-Top-Event-Categories • fwb-event-Top-Event-Types • fwb-event-Top-Login-By-User

Figure 246 shows the default report and edit report page.

Figure 246: Default report page



The following settings are available:

Step 1: Configure Report Settings	
Report Name	The template report name.
Time Period	Select the time period from the drop-down list. When selecting *Other*, you can specify the start and end date and time.
Devices	Select either *Specify* to add specific devices or select *All FortiGates, All FortiMails* or *All FortiWebs*.
Type	Select either *Single Report (Group Report)* or *Multiple Reports (Per-Device)*.
Output Profile (Notification)	Select the output profile from the drop-down list or select *Create New* to create a new output profile.
Color Code	Select a color code to apply to the report schedule.
Filters (Optional)	
Log messages that match	Select to match all filters or any of the following conditions.
(+) Add Filter	Select to add report filters. Select the field, operator, and value from the drop-down list. These filters will vary based on device type.
LDAP Query	Select the checkbox to add an LDAP query. Select the LDAP server from the drop-down list. Select the case change value from the drop-down list.

Language & Print Options (Optional)	
Language	Select the report language from the drop-down list.
Print Cover Page	Select the checkbox to print the report cover page. When selecting to print the cover page, you can customize the report cover page.
Print Table of Contents	Select the checkbox to print a table of contents.
Print Device List	Select the checkbox to print the device list. Select either *Compact*, *Count*, or *Detailed* from the drop-down list.
Obfuscate User	Select the checkbox to hide user information.
Step 2: Define Report Template	
Edit Template	Select *Edit Template* to edit report layout including headings, images, charts, and report settings.
Edit Cover Page	Select *Edit Cover Page* to edit cover page images, text, color, creation date, and data range. *Note:* You must select to *Print Cover Page* in step 1 for this option to be displayed.
Step 3: Schedule Report	
Enable Schedule	Select to enable schedules for the report selected.
Generate PDF Report Every	Select a time period from the drop-down list.
Starts on	Select the report start date.
End	Click the text field and select the report end date in the pop-up calendar.
Allow save maximum	Select a value between 1-10000 for the maximum number of reports to save.
Apply	Select to apply changes to the report template.
Reports	Reports are displayed in the lower content pane.
Run Now	Select to run the report now. The report in PDF format will be displayed in the bottom *Report* content pane.
Delete	Select reports and then select *Delete* from the toolbar.
Download	Select reports and then select *Download* from the toolbar.
Name	The name of the report.
Time	The time and date that the report was run.
Device Type	The device type that the report was run against.
Right-Click Menu	

Report	
Create New	Create a new report template.
Clone	Clone the report template selected.
Delete	Delete the report template. The default report templates cannot be deleted.
Import	Import a report template.
Export	Export a report template.
Go To Template	Go to the report template.
Folder	
Create New	Create a new template folder.
Rename	Rename a template folder.
Delete	Delete a template folder. Any report templates in the folder will be deleted.
Reports	
Run Now	Select to run the report now. The report in PDF format will be displayed in the bottom *Report* content pane.
Delete	Select reports and then select *Delete* from the toolbar.
Download	Select reports and then select *Download* from the toolbar.
Select All	Select *Select All* to select all reports in the lower reports content pane.

Configure reports

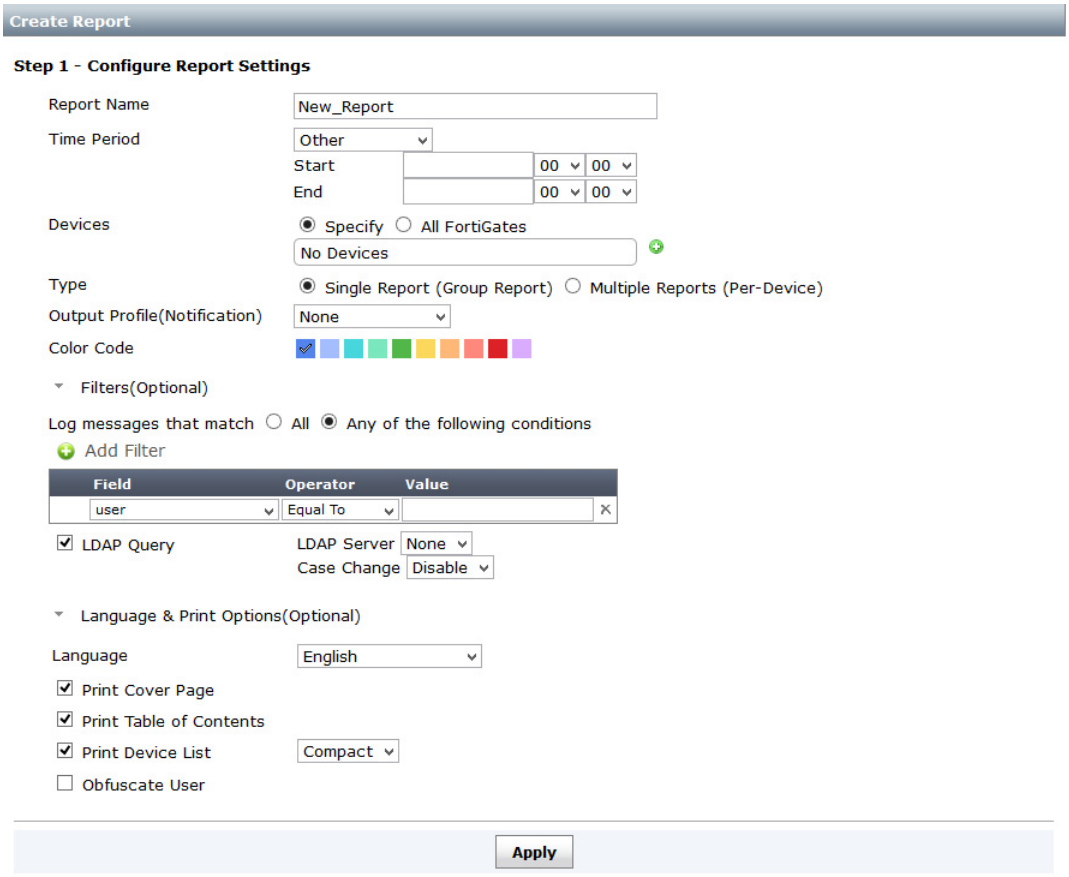
Reports and report templates can be created, edited, cloned, and deleted. You can also import and export report templates. New content can be added to and organized on a template, including: new sections, three levels of headings, text boxes, images, charts, and line and page breaks.

To create a new report template:

1. Go to the *Reports* tab and right-click on *Reports* in the tree menu.
2. In the right-click menu, under the *Report* heading, select *Create New*.

   The *Create Report* page opens.

Figure 247: Create report page



3. In the *Create Report* page, configure report settings. For more information see "Step 1: Configure Report Settings" on page 403.

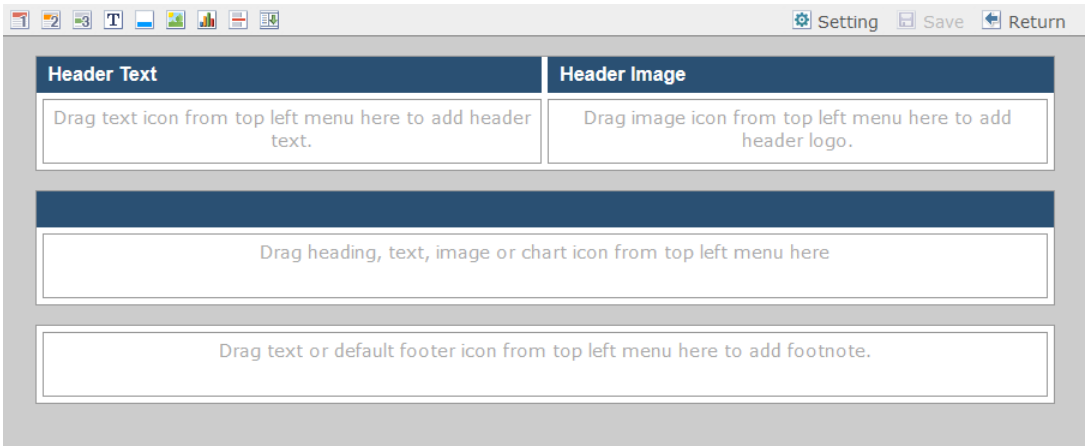


To create a custom cover page, you must select *Print Cover Page* in the *Language & Print Options* menu.

4. Select Apply to save the settings. *Step 2 - Define Report Template* and *Step 3 - Schedule Report* menu options are now available.
5. In the *Define Report Template* section, select *Edit Template*.

   The template page opens

Figure 248: Template page



6. In the *Template* page you can edit the report layout, add headers, text fields, images, and charts. Alternatively, you can right-click the report name and select *Go To Template* from the menu. For more information on template elements, see "Add report template content" on page 408.
7. Select *Setting* in the template toolbar to edit workspace and select *OK* to save changes. For more information. see "To edit the workspace of a report template:" on page 419.
8. Select *Save* in the template toolbar to save changes made to the report template. Select *Return* in the template toolbar to return to the *Create Report* page.
9. In the *Define Report Template* section, select *Edit Cover Page.* For more information, see "To edit cover page settings:" on page 417.
10. Select *Save* in the template toolbar to save the new report cover page. Select *Return* in the template toolbar to return to the *Create Report* page.
11. Configure report schedule. For more information, see "Step 3: Schedule Report" on page 404.
12. Select *Apply* to save the report template.

To clone a report template:

1. Go to the *Reports* tab and right-click on the report you would like to clone in the tree menu.
2. In the right-click menu, under the *Report* heading, select *Clone*.
3. In the *Clone Report Template* dialog box, enter a name for the new template, and select *OK*.

   A new template with the same information as the original template is created with the given name. You can then modify the cloned report as required.

To export a report template:

1. Go to the *Reports* tab and right-click on the report you would like to export in the tree menu.
2. In the right-click menu, under the *Report* heading, and select *Export*.
3. In the pop-up dialog box, select to save the file (.dat) to your management computer, and select *OK*. You can then import the report template to another FortiManager device.

To import a report template:

1. Go to the *Reports* tab and right-click on *Reports*.
2. In the right-click menu, under the *Report* heading, and select *Import*.
3. In the *Import Report Template* dialog box, select *Browse* and locate the report template (.dat) file on your management computer, and select *OK*. The report template will be loaded into FortiManager.

To create a new report template folder:

1. Go to the *Reports* tab and right-click on *Reports* in the tree menu.
2. In the right-click menu, under the *Folder* heading, and select *Create New*.
3. In the *Create New Folder* dialog box, enter a name for the folder, and select *OK*.

   A new template folder is created with the given name.

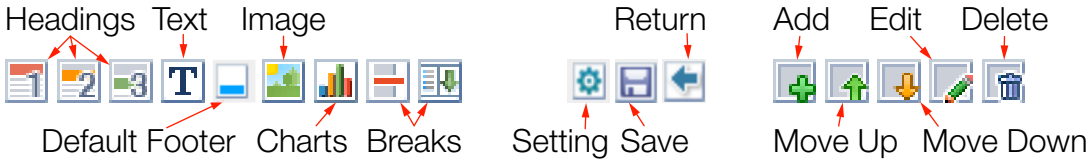
To delete a report template or report template folder:

1. Go to the *Reports* tab and right-click on the report template or report template folder that you would like to delete in the tree menu.
2. In the right-click menu select *Delete*.
3. In the confirmation dialog box, select *OK* to delete the report template or folder.

Add report template content

Various content can be added to a report template, such as charts, images, and typographic elements, using the section and template toolbars.

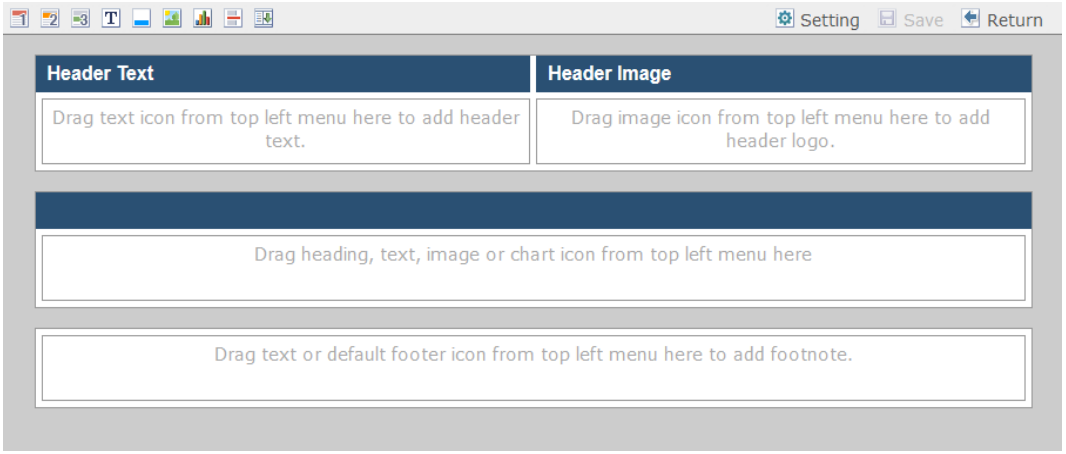
Figure 249: Template and section toolbars



To add a section to a report template:

1. Go to the *Reports* tab and select the report from the tree menu to which you would like to add content.
2. Select *Go To Template* in the right-click menu to display the report template.

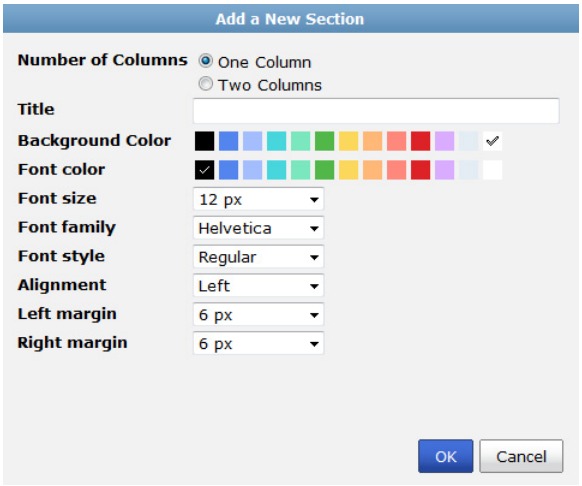
   Figure 250: Default new report



3. From the section toolbar, select the *Add* icon.

   The *Add a New Section* dialog box opens.

Figure 251: Add a new section



4. Configure the following settings:

Number of Columns	Select to display either one or two columns.
Title	Enter the section title.
Background Color	Select the background color from the palette.
Font color	Select the font color from the palette.
Font size	Enter the font size. The default is 12 px.
Font family	Select one of the following: *Courier, Helvetica, Times, SimSun, SimHei, MingLiu, MS-Gothic, MS-PGothic, MS-Mincyo, MS-PMincyo, DotumChe, Dotum, BatangChe*, or *Batang*.
Font style	Select one of the following: *Regular, Bold, Italic*, or *Bold and Italic*.
Alignment	Select one of the following: *Left, Center,* or *Right*.
Left margin	Select the left margin value from the drop-down list.
Right margin	Select the right margin value from the drop-down list.

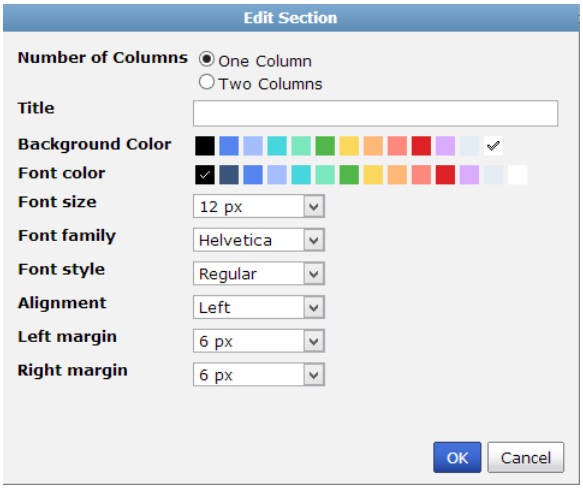
5. Select *OK* to create the new section.
6. If you are finished editing the template, select *Save* in the template toolbar to save your changes.
7. Select *Return* in the toolbar to return to *Create Report* page.

To edit a section in a report template:

1. Go to the *Reports* tab and select the report from the tree menu to which you would like to edit.
2. Select *Go To Template* in the right-click menu to display the report template.
3. From the section toolbar, select the *Edit Section* icon.

   The *Edit Section* dialog box opens.

Figure 252: Edit section



4. Configure the following settings:

Number of Columns	Select to display either one or two columns.
Title	Enter the section title.
Background Color	Select the background color from the palette.
Font color	Select the font color from the palette.
Font size	Enter the font size. The default is 12 px.
Font family	Select one of the following: *Courier, Helvetica, Times, SimSun, SimHei, MingLiu, MS-Gothic, MS-PGothic, MS-Mincyo, MS-PMincyo, DotumChe, Dotum, BatangChe*, or *Batang*.
Font style	Select one of the following: *Regular, Bold, Italic*, or *Bold and Italic*.
Alignment	Select one of the following: *Left, Center,* or *Right*.
Left margin	Select the left margin value from the drop-down list.
Right margin	Select the right margin value from the drop-down list.

5. Select *OK* to create the new section.
6. If you are finished editing the template, select *Save* in the template toolbar to save your changes.
7. Select *Return* in the toolbar to return to *Create Report* page.

To add header text to the report template:

1. Go to the *Reports* tab and select the report from the tree menu to which you would like to add a default header.
2. Select *Go To Template* in the right-click menu to display the report template.

3. Click and drag the text icon to the report header text field.



The header text and header image will print the cover page information including the device hostname in the report header when selecting not to print the report cover page in *Language & Print Options*.

4. If you are finished editing the template, select *Save* in the template toolbar to save your changes.
5. Select *Return* in the toolbar to return to *Create Report* page.

To add a default footer to report template footer:

1. Go to the *Reports* tab and select the report from the tree menu to which you would like to add a default header.
2. Select *Go To Template* in the right-click menu to display the report template.
3. Click and drag the default footer icon to the report footer.



The default header will print the cover information including the device hostname in the report header when selecting not to print the report cover in *Advanced Settings*.

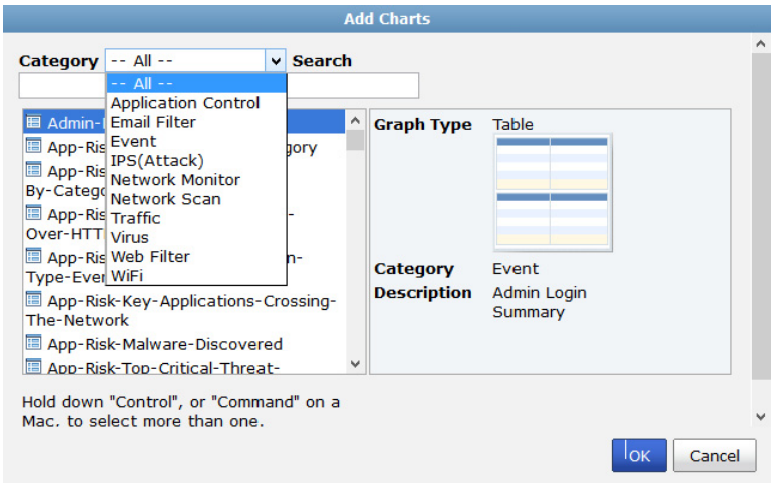
4. If you are finished editing the template, select *Save* in the template toolbar to save your changes.
5. Select *Return* in the toolbar to return to *Create Report* page.

To add a chart to a report template:

1. Go to the *Reports* tab and select the report from the tree menu to which you would like to add a chart.
2. Select *Go To Template* in the right-click menu to display the report template.
3. Click and drag the chart icon to the location where you want to add the chart.

   When you release the mouse button, the *Add Charts* dialog box will open.

Figure 253: Add a new chart

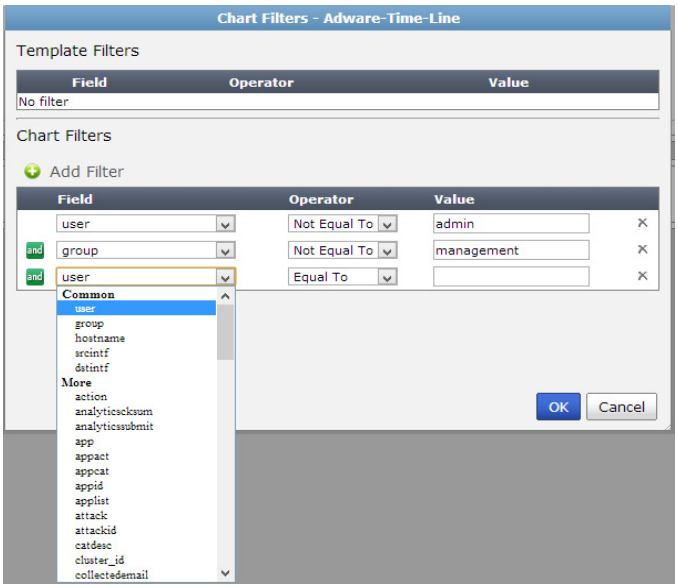


4. Find the chart that you would like to add in one of the following ways:
   - Browse the list of all the available the available charts.
   - Select the category of the chart you are looking for and then browse the list of the charts in that category.
   - Search for the chart by entering all or part of the chart name into the *Search* field.
5. Select *OK* once you have selected the chart you would like to add.

   The chart's placeholder will appear in the location that you had selected in the template.
6. To add a chart filter, select the filter icon.

   The *Chart Filters* dialog box will open.

Figure 254: Chart filters dialog box



7. If you are finished editing the template, select *Save* in the template toolbar to save your changes.
8. Select *Return* in the toolbar to return to *Create Report* page.



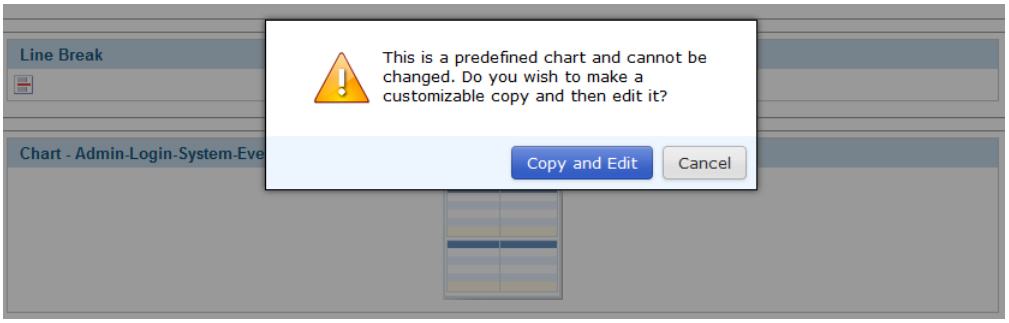
Although you can add filters to the predefined charts, you can not edit default predefined charts. When selecting to edit the chart, you will be prompted with a warning dialog box. You have the option to copy the chart and then make changes. The copy will replace the predefined chart in the report template.

To edit a predefined chart in a report template:

1. Go to the *Reports* tab and select the report from the tree menu to which you would like to add a chart.
2. Select *Go To Template* in the right-click menu to display the report template.
3. In the chart you want to edit, select the *Edit* icon in the chart toolbar.

   A warning dialog box is displayed.

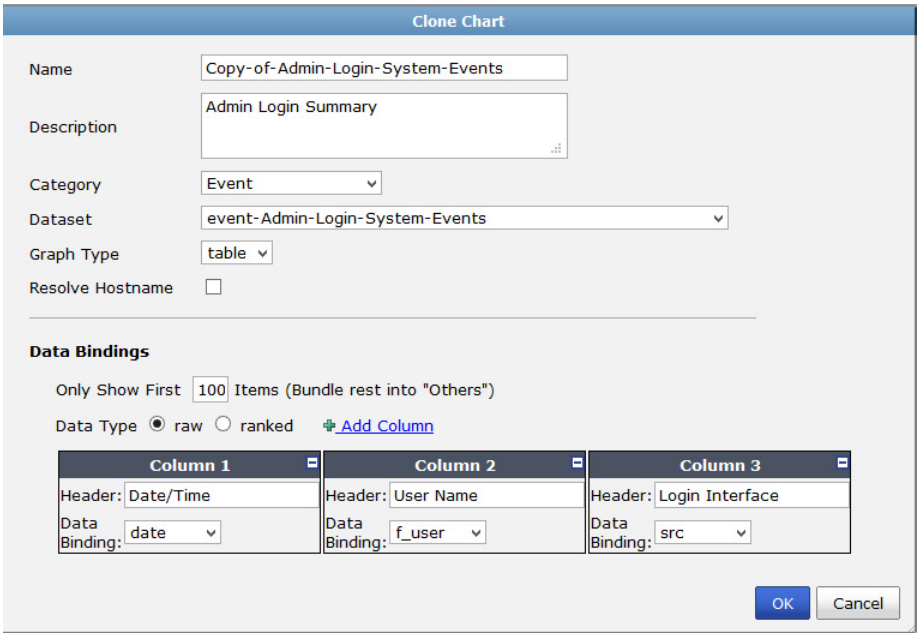
Figure 255: Edit predefined chart



4. Select the *Copy and Edit* button.

   The *Clone Chart* page is displayed.

Figure 256: Clone chart



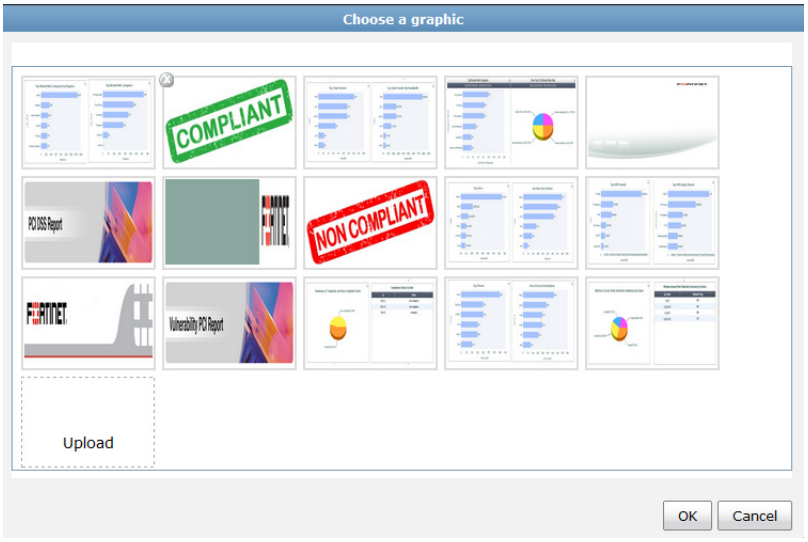
5. Edit the chart as required and select *OK* to save the changes. The copy will replace the predefined chart in the report template. The default name for a cloned chart is *Copy-of-Original-Chart-Name*.
6. If you are finished editing the template, select *Save* in the template toolbar to save your changes.
7. Select *Return* in the toolbar to return to *Create Report* page.

To add an image to a report template:

1. Go to the *Reports* tab and select the report from the tree menu to which you would like to add an image.
2. Select *Go To Template* in the right-click menu to display the report template.
3. Click and drag the image icon to the location where you want to add the image.

   The *Choose a graphic* dialog box will open.

Figure 257: Choose a graphic dialog box



4. Select an image from the list, or select *Upload* to browse for an image on your computer.
5. Select *OK* once you have selected the image you would like to add.

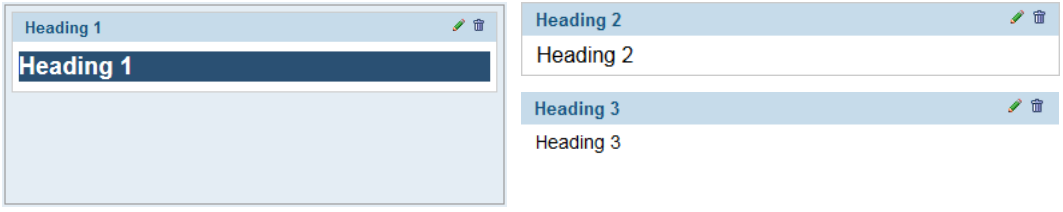
   The image will appear in the location that you had selected in the template.
6. If you are finished editing the template, select *Save* in the template toolbar to save your changes.
7. Select *Return* in the toolbar to return to *Create Report* page.

To add headings to a report template:

1. Go to the *Reports* tab and select the report from the tree menu to which you would like to add headings.
2. Select *Go To Template* in the right-click menu to display the report template.
3. Click and drag the required heading icon to the location where you want to add the template heading.

   When you release the mouse button, the selected element will be placed into the template.

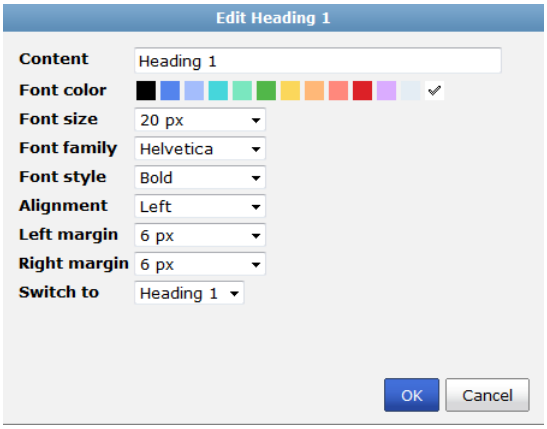
Figure 258: Heading element



4. To edit the heading text and level, select the edit icon on the template element, or double-click on the element.

   The *Edit Heading* dialog box will open.

Figure 259: Edit heading dialog box



5. Configure the following settings:

Content	Enter the heading text.
Font color	Select the font color from the palette.
Font size	Enter the font size.
Font family	Select one of the following: *Courier, Helvetica, Times, SimSun, SimHei, MingLiu, MS-Gothic, MS-PGothic, MS-Mincyo, MS-PMincyo, DotumChe, Dotum, BatangChe*, or *Batang*.
Font style	Select one of the following: *Regular, Bold, Italic*, or *Bold and Italic*.
Alignment	Select one of the following: *Left, Center,* or *Right*.
Left margin	Select the left margin value from the drop-down list.
Right margin	Select the right margin value from the drop-down list.
Switch to	Select to change the heading type.

6. Select *OK* to finish editing the heading.
7. If you are finished editing the template, select the *Save* icon to save your changes.
8. Select *Return* in the toolbar to return to *Create Report* page.

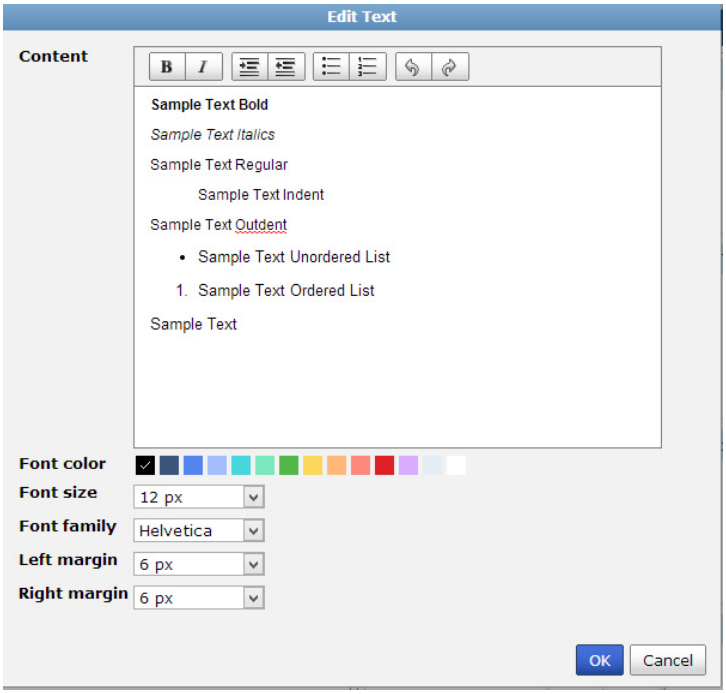
To add text to a report template:

1. Go to the *Reports* tab and select the report from the tree menu to which you would like to add text.
2. Select *Go To Template* in the right-click menu to display the report template.
3. Click and drag the text icon to the location where you want to add the text box.

   When you release the mouse button, the selected element will be placed into the template.
4. To edit the text, select the edit icon on the template element, or double-click on the element.

   The *Edit Text* dialog box will open.

Figure 260: Edit text dialog box



5. Configure the following settings:

Content	Enter the text in this text field. You can change text elements in the text toolbar. The following options are available: bold, italics, indent, outdent, unordered list (bullets), ordered list (numbered list), undo, and redo. Use the right-click menu to cut, copy, paste, and delete content. You can also configure languages and the spell checker.
Font color	Select the font color from the palette.
Font size	Enter the font size. The default size is 12 px.
Font family	Select one of the following: *Courier, Helvetica, Times, SimSun, SimHei, MingLiu, MS-Gothic, MS-PGothic, MS-Mincyo, MS-PMincyo, DotumChe, Dotum, BatangChe*, or *Batang*.
Font style	Select one of the following: *Regular, Bold, Italic*, or *Bold and Italic*.
Left margin	Select the left margin value from the drop-down list.
Right margin	Select the right margin value from the drop-down list.

6. Select *OK* to finish editing the text.
7. If you are finished editing the template, select *Save* in the template toolbar to save your changes.

8. Select *Return* in the toolbar to return to *Create Report* page.



When adding text to the report header or footer, you can only edit the content. Additional settings are not available for the text element in the report header or footer.



It is recommended to edit the section prior to adding text elements as the section menu will override settings in an existing custom text section.

To add breaks to a report template:

1. Go to the *Reports* tab and select the report from the tree menu that you would like to edit.
2. Select *Go To Template* in the right-click menu to display the report template.
3. Click and drag the required break icon to the location where you want to add the break. Line breaks and page breaks are available.

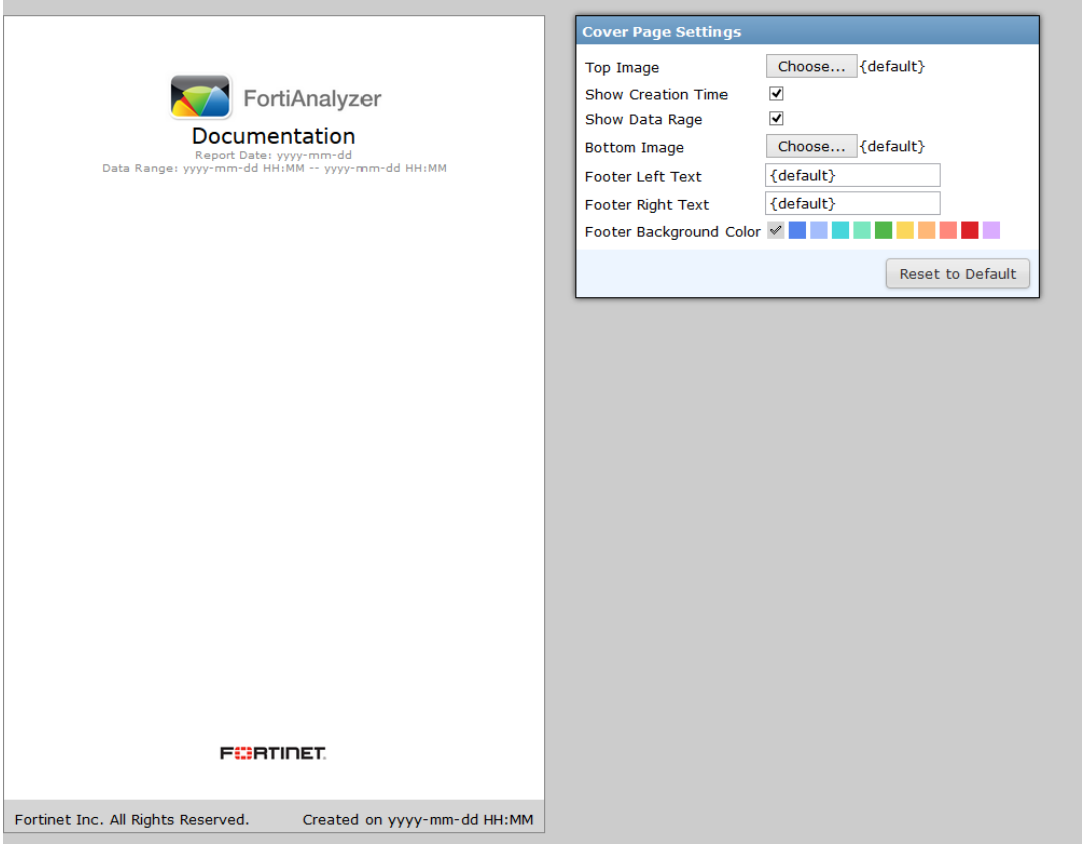
   When you release the mouse button, the selected break will be placed into the template.
4. If you are finished editing the template, select *Save* in the template toolbar to save your changes.
5. Select *Return* in the toolbar to return to *Create Report* page.

To edit cover page settings:

1. Go to the *Reports* tab and select the report from the tree menu that you would like to edit.
2. Select *Edit Cover Page* in the *Define Report Template* section.

   The *Cover Page Settings* page opens.

Figure 261: Cover Page Settings page



3. Configure the following settings:

Top Image	Select *Choose* to select an image or upload a new image. Select an image in the pop-up window and select *OK* to save the selection.
Show Creation Time	Select the checkbox to print the report date on the cover page.
Show Data Range	Select the checkbox to print the data range on the cover page.
Bottom Image	Select *Choose* to select an image or upload a new image. Select an image in the pop-up window and select *OK* to save the selection.
Footer Left Text	Select to edit the text printed in the left hand footer of the cover page.
Footer Right Text	Select to edit the text printed in the left hand footer of the cover page.
Footer Background Color	Select the cover page footer background color from the palette.
Reset to Default	Select to reset the cover page settings to their default settings.

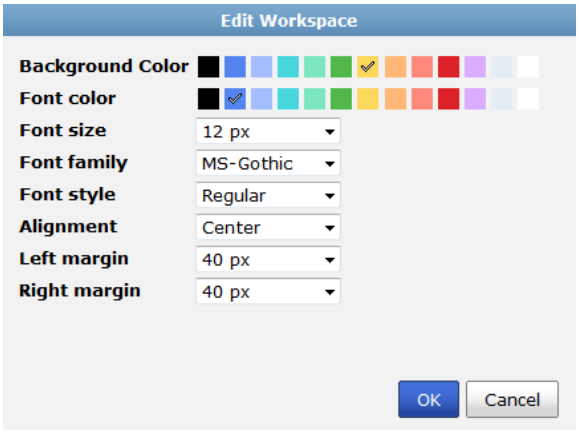
4. Select the *Save* button in the toolbar to save changes and select the *Template* button to return to the report template page.
5. Select *Return* in the toolbar to return to *Create Report* page.

To edit the workspace of a report template:

1. Go to the *Reports* tab and select the report from the tree menu that you would like to edit.
2. Select *Go To Template* in the right-click menu to display the report template.
3. Select *Setting* in the template toolbar.

   The *Edit Workspace* window opens.

Figure 262: Edit workspace window



4. Configure the following settings:

Background Color	Select the background color from the palette.
Font color	Select the font color from the palette.
Font size	Enter the font size. The default size is 12 px.
Font family	Select one of the following: *Courier, Helvetica, Times, SimSun, SimHei, MingLiu, MS-Gothic, MS-PGothic, MS-Mincyo, MS-PMincyo, DotumChe, Dotum, BatangChe*, or *Batang*.
Font style	Select one of the following: *Regular, Bold, Italic*, or *Bold and Italic*.
Alignment	Select one of the following: *Left, Center,* or *Right*.
Left margin	Select the left margin value from the drop-down list.
Right margin	Select the right margin value from the drop-down list.

5. If you are finished editing the template, select *Save* in the template toolbar to save your changes.
6. Select *Return* in the toolbar to return to *Create Report* page.

Edit report template content

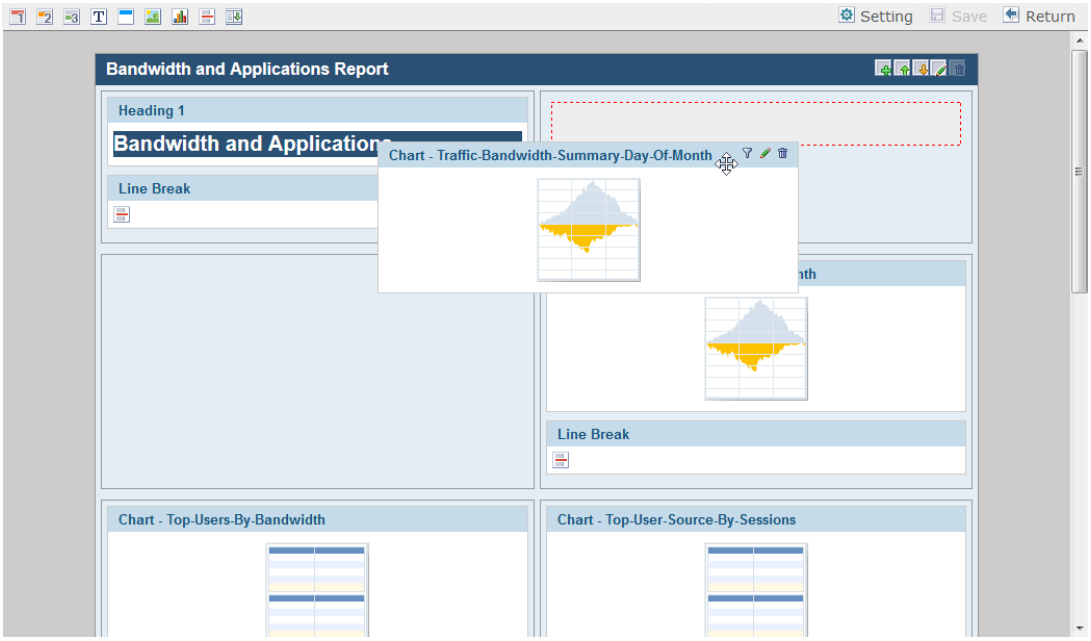
The elements added to report template can be moved, deleted, and some of them can be edited.

To move a report template element:

1. Go to the *Reports* tab and select the report from the tree menu that you would like to edit.
2. Select *Go To Template* in the right-click menu to display the report template.
3. Click and drag an element to the desired location.

   A gray box with a dashed red outline will appear in the location where the element will be placed.
4. Release the mouse button to drop the element into the desired location.

Figure 263: Move a report template element



5. When you are finished editing the template, select *Save* in the template toolbar to save your changes.

To edit a report template element:

1. Go to the *Reports* tab and select the report from the tree menu that contains to the element you would like to edit.
2. Select *Go To Template* in the right-click menu to display the report template.
3. Select the edit icon in top right corner of the element to be edited. Break elements cannot be edited.

Figure 264: Edit an element



4. Depending on the type of element you are editing, an appropriate edit dialog box will open.

   The edit element dialog boxes contain the same information as the add element dialog boxes, see "Add report template content" on page 408.
5. When you have completed the required edits, select *OK* to close the edit element dialog box.
6. Select *Save* in the template toolbar to save your changes.

To delete a report template element:

1. Go to the *Reports* tab and select the report from the tree menu that contains to the element you would like to delete.
2. Select *Go To Template* in the right-click menu to display the report template.
3. Select the delete icon in the top right corner of the element.
4. Select *OK* in the confirmation dialog box to delete the element.
5. Select *Save* in the template toolbar to save your changes.

Import and export report templates

Report templates can be imported from and exported to the management computer.

To import a report template:

1. Go to the *Reports* tab and right-click on a report in the tree menu.
2. Select *Import* in the pop-up menu.

   The *Import Report Template* dialog box opens.
3. Select *Browse* and browse to the location of the template file.
4. Select *OK* to import the report template.

To export a report template:

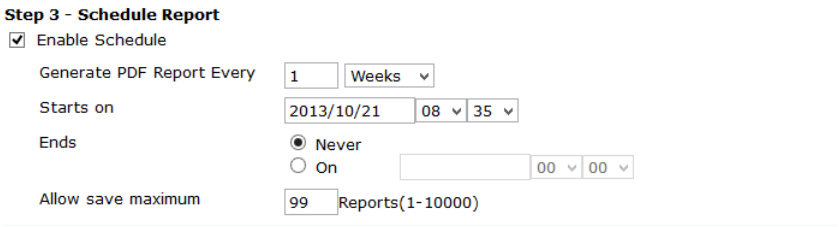
1. Go to the *Reports* tab and right-click on a report in the tree menu.
2. Select *Export* in the pop-up menu.
3. Select a location to save the template, then select *OK* to export the report template.

Schedules

Report schedules provide a way to schedule an hourly, daily, weekly, or monthly report so that the report will be generated at a specific time. You can also manually run a report schedule at any time and enable or disable report schedules.

The schedule is built-in to the report template.

Figure 265: Schedule a report template



Configure the following settings:

Enable Schedule	Select to enable report template schedules.
Generate PDF Report Every	Select when the report is generated: • Enter a number for the frequency of the report based on the time period selected from the drop-down list, or select *On Demand* to only run the report manually. • If *On Demand* is not selected, enter a starting and ending date and time for the file generation, or set it for never ending.
Starts On	Enter a starting date and time for the file generation.
Ends	Enter an ending date and time for the file generation, or set it for never ending.
Allow save maximum	Select a value between 1-10000 for the maximum number of reports to save.

To edit a report schedule:

1. Go to the *Reports* tab and right-click a report in the tree menu.
2. Edit the report schedule as required and select *Apply* to apply the changes.

To delete a scheduled report:

1. Go to the *Reports* tab and select *Report Calendar* in the tree menu.
2. Right-click the scheduled report you would like to delete and then select *Delete* from the pop-up menu.
3. Select *OK* in the confirmation dialog box to delete the scheduled report.

To manually run a report:

1. Go to the *Reports* tab and select a report in the tree menu.
2. Select *Run Now* from the report toolbar in the lower content pane to run the report. Optionally, you can select *Run* in the template toolbar.

   The report will run and the report will be generated and listed under *Latest Reports*. See "Reports" on page 424 for information on viewing the report.

To disable a scheduled report:

1. Go to the *Reports* tab and select *Report Calendar* in the tree menu.
2. Right click the scheduled report and select *Disable* from the right-click menu.
3. In the confirmation box, select *OK*.

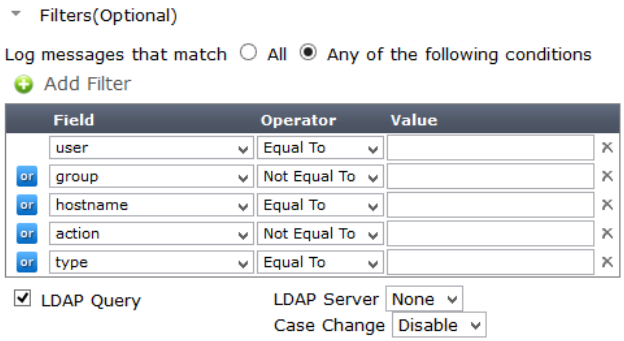


Disabling a report will remove all scheduled instances of the report from the report calendar. Completed reports will remain in the report calendar.

Filters

In the filters section of the *Configure Report Settings* section, you can apply filters and add an LDAP query.

Figure 266: Report filters



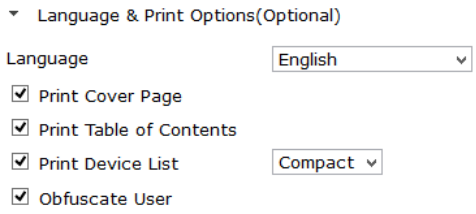
Configure the following settings

Log messages that match	Select to apply all filters or any of the selected filters.
Add Filter	Select the Add Filter icon to add a filter to the report. Select the field, operator, and enter a value in the text field.
LDAP Query	Select to add an LDAP query to the report. Select the LDAP server from the drop-down list. Select to enable or disable case change.

Language & Print options

In the *Language & Print Options* section of the report, you can further customize reports. You can configure report language, print the cover page, print the table of contents, print a device list, and obfuscate users.

Figure 267: Language & Print Options



Configure the following settings:

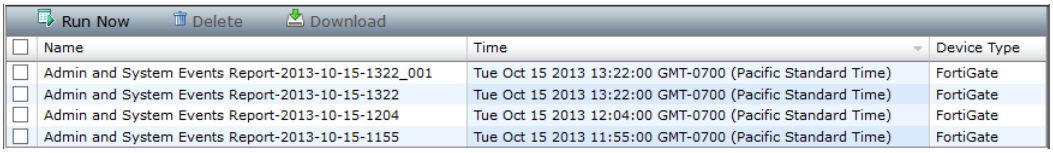
Language	Select the report language. Select one of the following: *English, French, Japanese, Korean, Portuguese, Simplified_Chinese, Spanish,* or *Traditional_Chinese*.
Print Cover Page	Select to print a report cover page.
Print Table of Contents	Select to print a table of contents.
Print Device List	Select to print the device list. Select one of the following: C*ompact, Count, Detailed*.
Obfuscate User	Select to obfuscate user names in the report.

Reports

Reports are displayed in the lower content pane. You can view reports that have been generated on the FortiManager system. This page displays the report name, the time and date that the report was generated, and the device type. Select a report from the list to view the report in a new window or tab in your web-browser.

The reports can also be downloaded as PDFs, and deleted.

Figure 268: Latest reports



To view the latest reports:

Latest reports can be viewed for a specific report template from the *Reports* tab or for a specific device from the *Device Manager* tab.

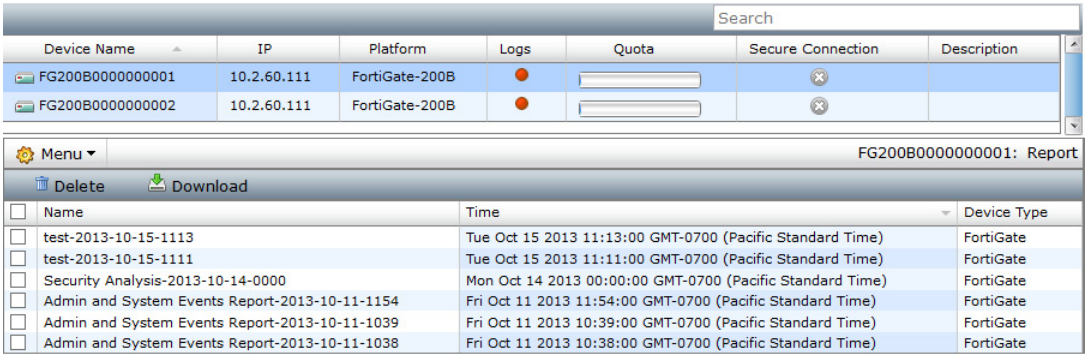
To view latest reports from the *Reports* tab:

1. Go to the *Reports* tab and select the report in the tree menu.
2. In the lower content pane you can select a report to view the report, delete the report or download the report.

To view latest reports from the *Device Manager* tab:

1. Go to the *Device Manager* tab and select the ADOM that contains the device whose latest report you would like to view.
2. The report history is shown in the lower content pane showing a list of all the reports that have been run for that device.

Figure 269: Device reports



To delete a report:

1. In the Reports content pane, select the checkbox in the right column beside the report name.
2. Select *Delete* in from the toolbar and select *OK* in the confirmation dialog box to delete the report or reports.

To delete multiple reports:

1. In the *Reports* content pane, select the checkbox for *Show All* to display all reports. The *Show All* link is displayed when 20 or more reports are in the *Latest Reports* list.
2. Select the checkbox beside the reports you would like to delete and select *Delete* in the toolbar. To select all reports, select *Select All* in the right-click menu and then select *Delete*.

To download reports:

1. In the *Reports* content pane, select the download icon in the right column beside the report name.
2. Save the file to your computer, or open the file in an applicable program.

To download multiple reports:

1. In the *Reports* content pane select *Show All* to display all reports. The *Show All* link is displayed when 20 or more reports are in the *Latest Reports* list.
2. Select the checkbox beside the reports you would like to download and select *Download* in the toolbar. To select all reports, select *Select All* in the right-click menu and then select *Download*.



You can also download and delete device reports in the *Device Manager* tab.

Chart library

The FortiManager unit provides a selection of predefined charts. New charts can be created using the new chart builder wizard, by cloning and editing an existing chart, or by using the advanced chart option. You can select to display predefined chart, custom charts, or both.

FortiManager v5.0 Patch Release 4 or later includes a chart builder wizard to enable you to create custom charts. For advanced users, right-click the right content pane and select *Create New* to create SQL based charts.

Chart builder wizard

To access the chart builder wizard, go to the *Reports* tab, select *Chart Library*, and select *Wizard* in the toolbar. To create a new chart, follow the steps listed below.

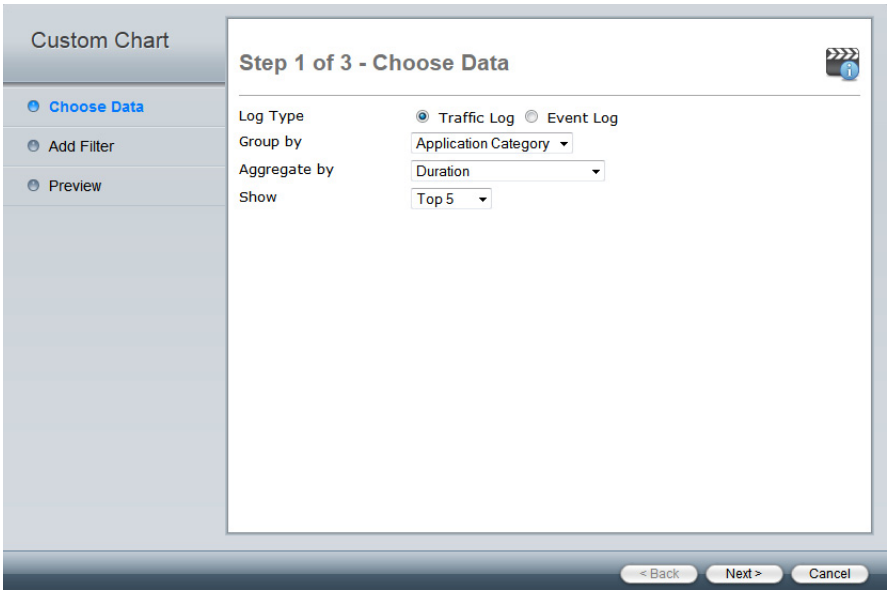


The chart builder wizard is available for FortiGate and FortiCarrier ADOMs only.

Step 1: Choose data

You can create charts for traffic or event logs.

Figure 270: Choose data page





Select the video icon to view the FortiManager 5.0: How to create a custom chart tutorial.

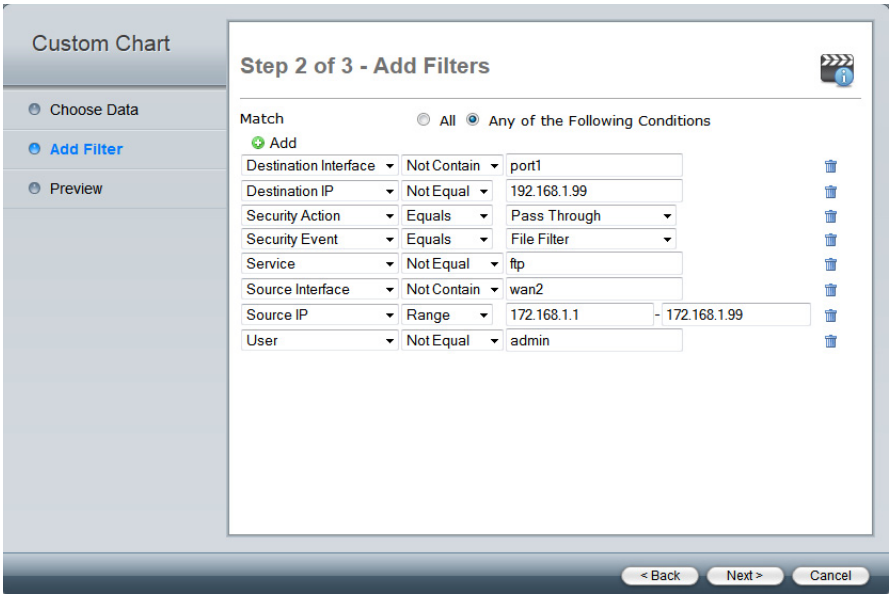
Configure the following settings:

Log Type	Select either *Traffic Log* or *Event Log*.
Group by	The options in the drop-down list are dependent on the log type selected. The *Group by* option will be displayed in the column 1 or Y-axis in the chart. Traffic log attributes: *Application Category, Application ID, Application Name, Attack, Destination Country, Destination Interface, Destination IP, Device Type, Source Interface, Source IP, Source SSID, User, Virus, VPN, VPN Type, Web Category*, or *Website (Hostname)*. Event log attributes: *VPN Tunnel* or *Remote IP*.
Aggregate by	Select one of the following from the drop-down list: *Duration, Received Bytes, Sent Bytes, Total Bytes*, *Total Sessions* or *Total Blocked Sessions*. The *Aggregate by* option will be displayed in the column 2 or X-axis in the chart.
Show	Select one of the following from the drop-down list: *Top 5, Top 10, Top 25, Top 50*, or *Top 100*.

Step 2: Add filters

You can add one or more filters to the chart and select to match all or any conditions. These filters will be permanently saved to the dataset query.

Figure 271: Add filters page



Configure the following settings:

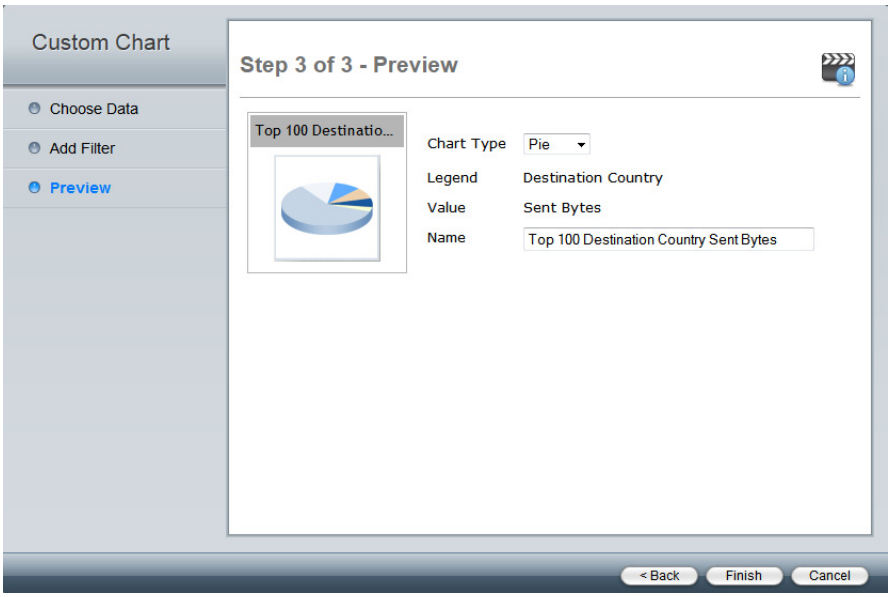
Match	Select to match all or any of the configured conditions.
+ Add	Select one of the following filter fields in the drop-down list:

Destination Interface	Select *Equals, Not Equal, Contains,* or *Not Contain* from the second drop-down list and enter a value in the text field. Select the garbage can icon to delete the filter. This filter is available for traffic logs only.
Destination IP	Select *Equals, Not Equal,* or *Range* from the second drop-down list. When selecting *Range*, enter the starting and ending IP address in the text fields. Select the garbage can icon to delete the filter. This filter is available for traffic logs only.
Security Action	Select *Equals or Not Equal* from the second drop-down list. Select *Pass Through* from the third drop-down list. Select the garbage can icon to delete the filter. This filter is available for traffic logs only.
Security Event	Select *Equals or Not Equal* from the second drop-down list. Select one of *Analytics, Application Control, AV Error, Banned Word, Command Block, DLP, File Filter, General Mail Log, HTML Script Virus, IPS, MIME Fragmented, MMS Checksum, MMS Dupe, MMS Endpoint, MMS Flood, MAC Quarantine, Oversize, Script Filter, Spam Filter, SSH Block SSH Log, Switching Protocols, Virus, VOIP, Web Content, Web Filter,* or *Worm* from the third drop-down list. Select the garbage can icon to delete the filter. This filter is available for traffic logs only.
Service	Select *Equals, Not Equal, Contains,* or *Not Contain* from the second drop-down list and enter a value in the text field. Select the garbage can icon to delete the filter. This filter is available for traffic and event logs.
Source Interface	Select *Equals, Not Equal, Contains,* or *Not Contain* from the second drop-down list and enter a value in the text field. Select the garbage can icon to delete the filter. This filter is available for traffic logs only.
Source IP	Select *Equals, Not Equal,* or *Range* from the second drop-down list. When selecting *Range*, enter the starting and ending IP address in the text fields. Select the garbage can icon to delete the filter. This filter is available for traffic logs only.
User	Select *Equals, Not Equal, Contains,* or *Not Contain* from the second drop-down list and enter a value in the text field. Select the garbage can icon to delete the filter. This filter is available for traffic and event logs.

Step 3: Preview

The preview page allows you to select the chart type and rename the custom chart.

Figure 272: Preview page



Configure the following settings:

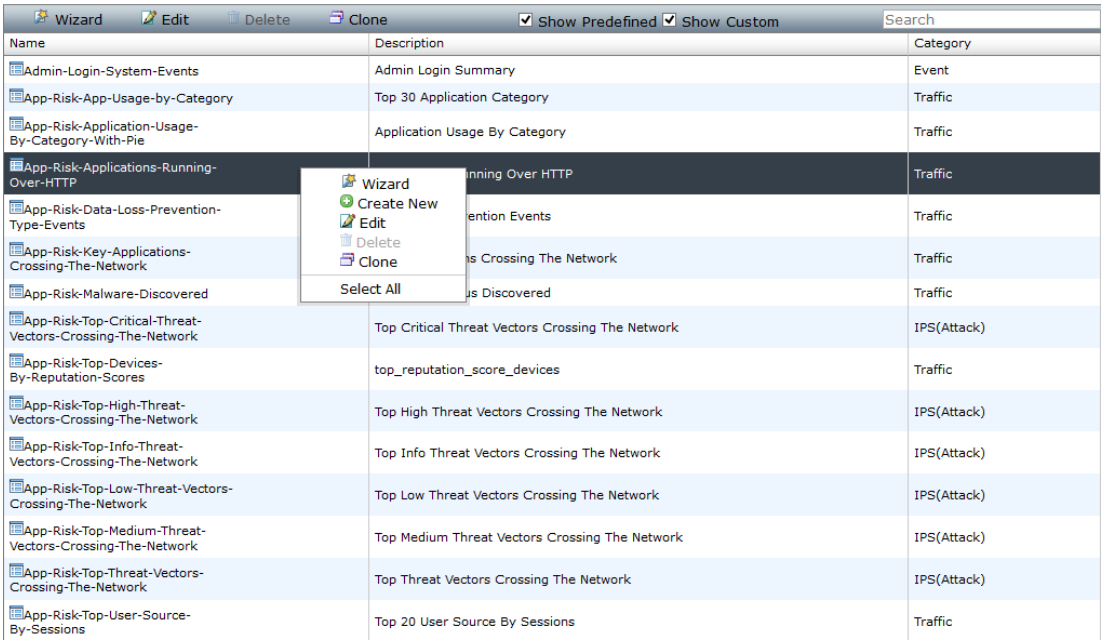
Chart Type	Select the chart type in the drop-down list. Select one of the following: *Table, Bar, Line*, or *Pie*. Note: Depending on the chart settings, you may not be able to change the chart type.
Column 1/Y-axis	Displays the *Group by* selection.
Column 2/X-axis	Displays the *Aggregate by* selection.
Name	Displays the default name of the custom chart. You can edit the name field.

Select *Finish* to add the custom chart. You can now apply the custom chart to a report template.

Advanced chart option

To view and configure charts, go to the *Reports* tab and select *Create New* in the right-click menu.

Figure 273: Charts page



The following options are available:

Wizard	Select to launch the chart builder wizard.
Edit	Select to edit a chart.
Delete	Select to delete a chart.
Clone	Select to clone an existing chart.
Show Predefined	Select to display predefined charts.
Show Custom	Select to display custom charts.
Search	Use the search field to find a specific chart.
Create New	Select *Create New* from the right-click menu to use the advanced chart builder.

Charts are predefined to show specific information in an appropriate format, such as pie charts or lists. They are organized into categories, and can be added to, removed from, and organized in reports. You can select to show predefined charts, custom charts, or both.



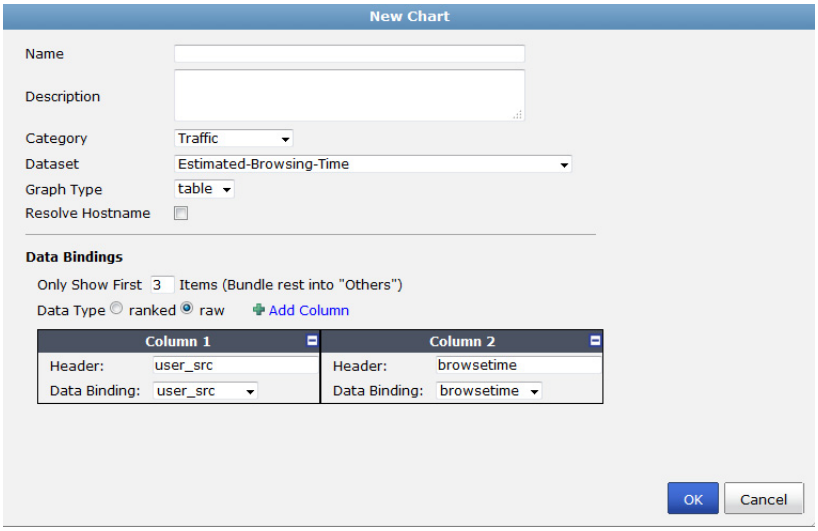
The available predefined charts may change. FortiManager v5.0 Patch Release 3 or later include enhanced charts for FortiGate and charts for FortiMail and FortiWeb.

To create a new chart:

1. Go to the *Reports* tab, select an existing chart, and select *Create New* in the right-click menu.

   The *New Chart* dialog box opens.

   Figure 274: Create new chart (table) dialog box



2. Enter the required information for the new chart.

Name	Enter a name for the chart.
Description	Enter a description.
Category	Select a category for the chart from the drop-down menu. Select one of the following: *Traffic, Event, FortiMail, IPS(Attack), Web Filter, Virus, Network Scan, Email Filter, FortiWeb,* or *WiFi*.
Dataset	Select a dataset from the drop-down list. See "Dataset" on page 434 for more information. These filters will vary based on device type.
Graph Type	Select a graph type from the drop-down list. Select one of the following: bar, pie, table, or line.
Resolve Hostname	Select to resolve the hostname.
bar, pie, or line	
Line Subtype	Select one of the following: *basic*, *stacked*, or *back-to-back*. This option is only available when *line* is selected as the graph type.
X-Axis	*Data Binding*: Select a value from the drop-down menu. *Only Show First*: Enter a numerical value. Only the first 'X' items will be displayed. Other items are bundled into Others. *Overwrite label*: Enter a label.
Y-Axis	*Order By*: Select a value from the drop-down menu. *Data Binding*: Select a value from the drop-down menu. *Overwrite label*: Enter a label.

Order By	Select to order by the X-Axis or Y-Axis. This option is only available when the graph type is line or bar.
table	
Only Show First Items	Enter a numerical value. Only the first 'X' items will be displayed. Other items are bundled into *Others*.
Data Type	Select either *ranked* or *raw*.
Columns	Up to fifteen columns can be included. *Header*: Enter header information. *Data Binding*: Select a value from the drop-down menu.
Add Column	Select to add a column.

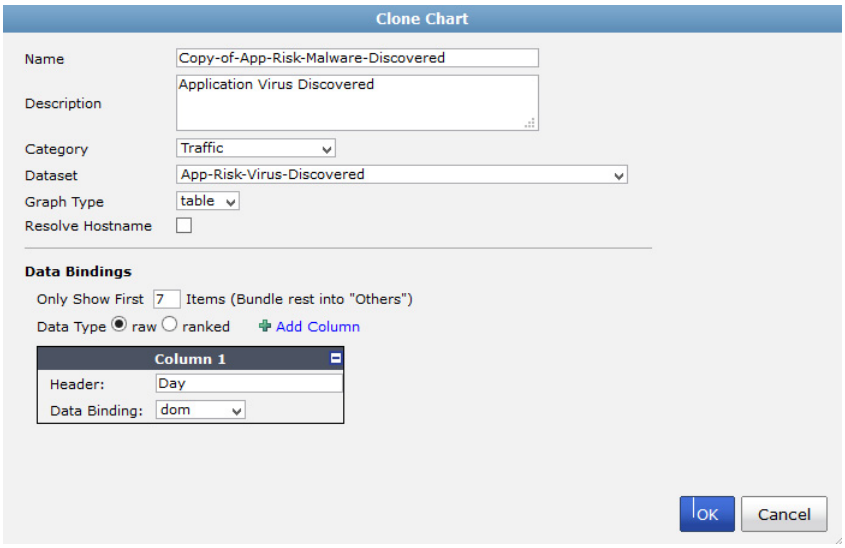
3. Select *OK* to create the new chart.

To clone a chart:

1. Go to the *Reports* tab and select *Chart* in the tree menu.
2. Select the chart that you would like to clone and select *Clone* from the toolbar or right-click menu.

   The *Clone Chart* dialog box opens.

Figure 275: Clone chart dialog box



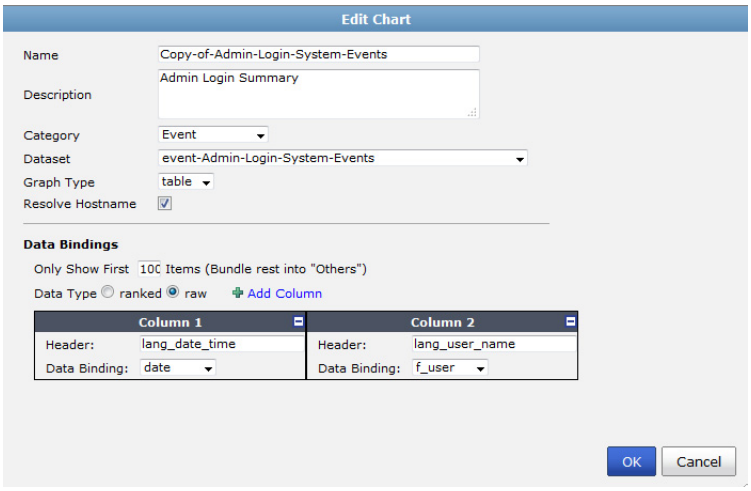
3. Edit the information as needed and select *OK* to clone the chart.

To edit a chart:

1. Go to the *Reports* tab and select *Chart* in the tree menu.
2. Double-click on the chart that you would like to edit, or select the chart and select *Edit* from the toolbar or right-click menu.

   The *Edit Chart* dialog box opens.

   Figure 276: Edit chart dialog box



3. Edit the information as required and select *OK* to finish editing the chart.



Predefined charts cannot be edited, the information is read-only. You can clone a predefined chart and make changed to the copy.

To delete charts:

1. Go to the *Reports* tab and select *Chart Library* in the tree menu.
2. Select the chart or charts that you would like to delete and select *Delete* from the toolbar or right-click menu.
3. Select *OK* in the confirmation dialog box to delete the chart or charts.



Predefined charts cannot be deleted, the information can only be viewed.

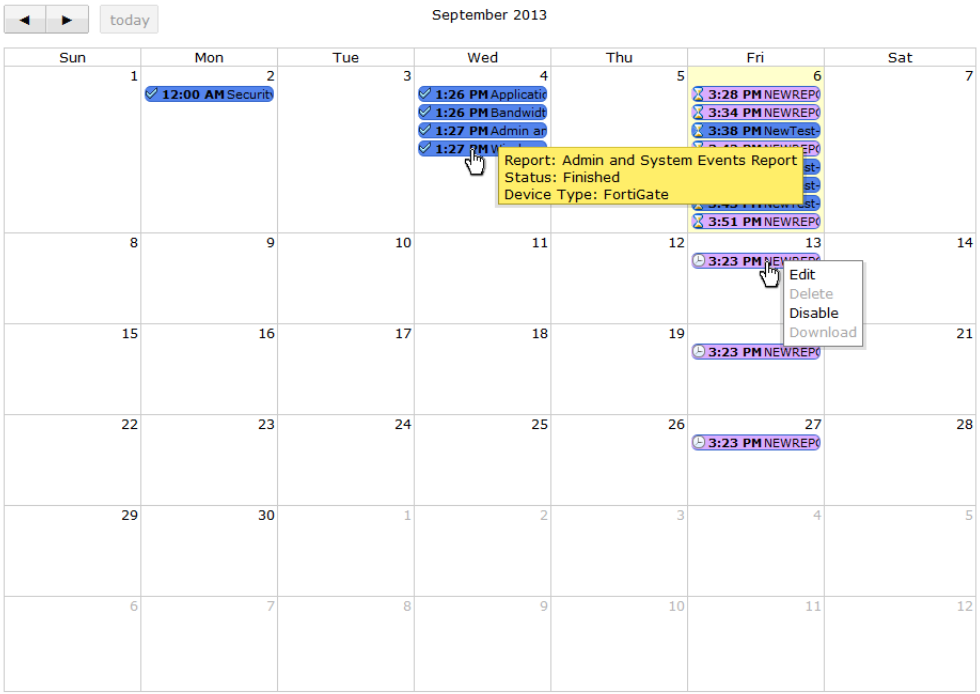
Report calendar

The report calendar provides an overview of scheduled reports. You can view all reports scheduled for the selected month.

Right-clicking a report schedule in the calendar, and selecting *Edit*, opens the *Edit Report* page, allowing you to make changes to the settings for that schedule (see "Schedules" on page 422). If the report has already been run, you can right-click the report schedule and select *Download* to download the report to your management computer.

To view the report calendar, go to the *Reports* tab and select *Report Calendar* in the tree menu.

Figure 277: Report calendar



When hovering the mouse cursor over a scheduled report on the calendar, a notification box will appear detailing the report name, status, and the device type.

Advanced

The advanced menu allows you to view, configure and test datasets, create output profiles, and report languages.

Dataset

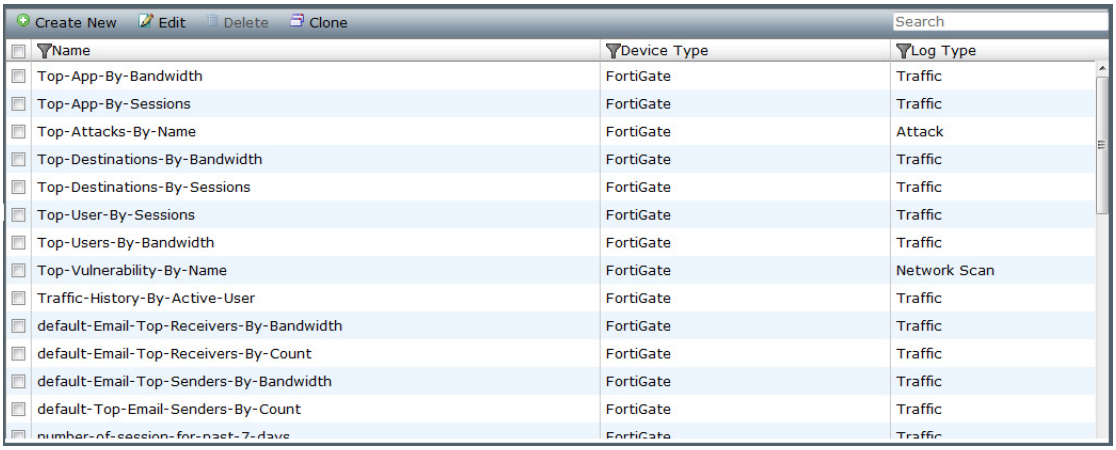
FortiManager datasets are collections of log files from monitored devices. Reports are generated based on these datasets. These filters will vary based on device type.

Predefined datasets for each supported device type are provided, and new datasets can be created and configured. FortiManager v5.0 Patch Release 2 or later adds the ability to test a SQL query per dataset against specific devices or log arrays before saving the configuration.

FortiManager v5.0 Patch Release 5 introduces new datasets for SIP and SCCP.

To view and configure datasets, go to the *Reports* tab and select *Advanced* > *Dataset* in the tree menu.

Figure 278: Datasets



The following options are available:

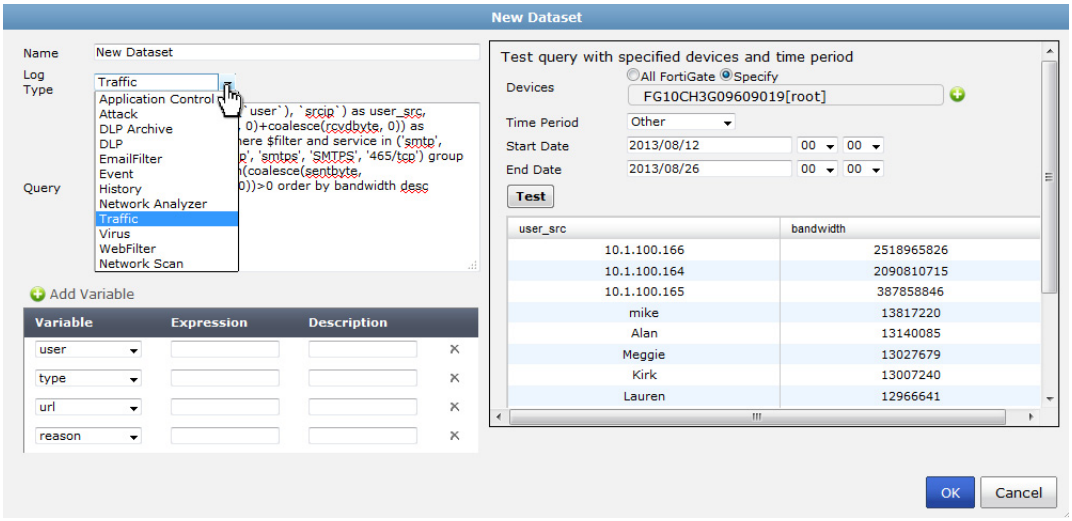
Create New	Select to create a new dataset.
Edit	Select to edit an existing dataset.
Delete	Select to delete a dataset.
Clone	Select to clone an existing dataset.
Search	Use the search field to find a specific dataset.

To create a new dataset:

1. Go to the *Reports* tab and select *Advanced* > *Dataset* in the tree menu.
2. Select *Create New* on the toolbar, or right-click in the dataset list and select *New* from the pop-up menu.

   The *Create New D*ataset dialog box opens.

Figure 279: New dataset dialog box



3. Enter the required information for the new dataset.

Name	Enter a name for the dataset.
Log Type	Select a log type from the drop-down list. The following log types are available for FortiGate: *Application Control, Attack, DLP Archive, DLP, Email Filter, Event, Traffic, Virus, Web Filter,* and *Network Scan*. The following log types are available for FortiMail: *Email Filter, Event, History,* and *Virus*. The following log types are available for FortiWeb: *Attack, Event,* and *Traffic*.
Query	Enter the SQL query used for the dataset.
Add Variable	Select to add a variable, expression, and description information.
Test query with specified devices and time period	Select devices and test the SQL query against the new dataset. In FortiManager v5.0 Patch Release 2 or later you can test the query against specific devices or a log array.
Devices	Select *All FortiGates, All FortiMails, All FortiWebs,* or *Specify* to select specific devices or log arrays to run the SQL query against.
Time Period	Use the drop-down menu to select a time period. When selecting Other, enter the start date, time, end date, and time.
Test	Select Test to test the SQL query before saving the dataset configuration.

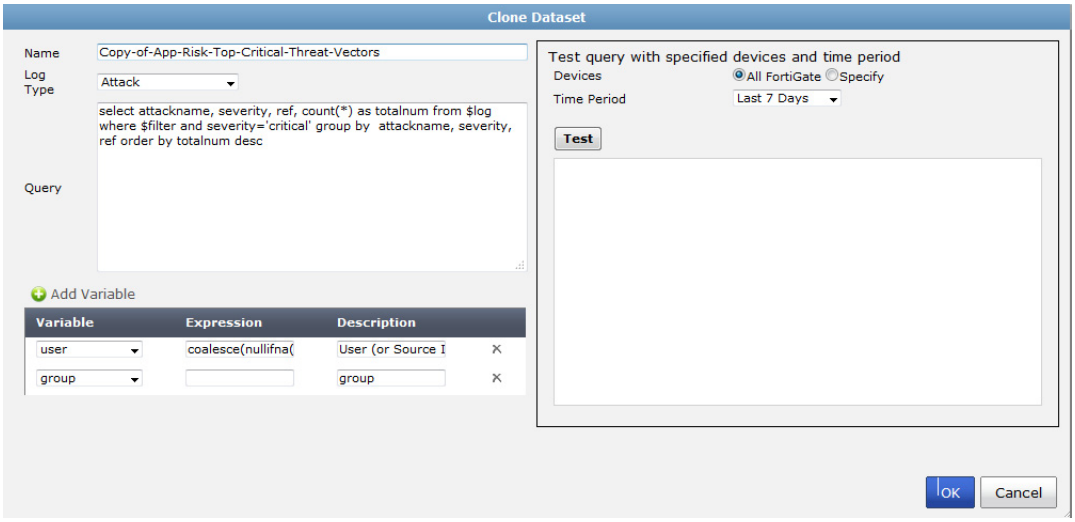
4. Test the query to ensure that the dataset functions as expected.
5. Select *OK* to create the new dataset.

To clone a dataset:

1. Go to the *Reports* tab and select *Advanced* > *Dataset* in the tree menu.
2. Select the dataset that you would like to clone and select *Clone* from the toolbar or right-click menu.

   The *Clone Dataset* dialog box opens.

Figure 280: Clone dataset dialog box



You can clone a predefined dataset or custom dataset.

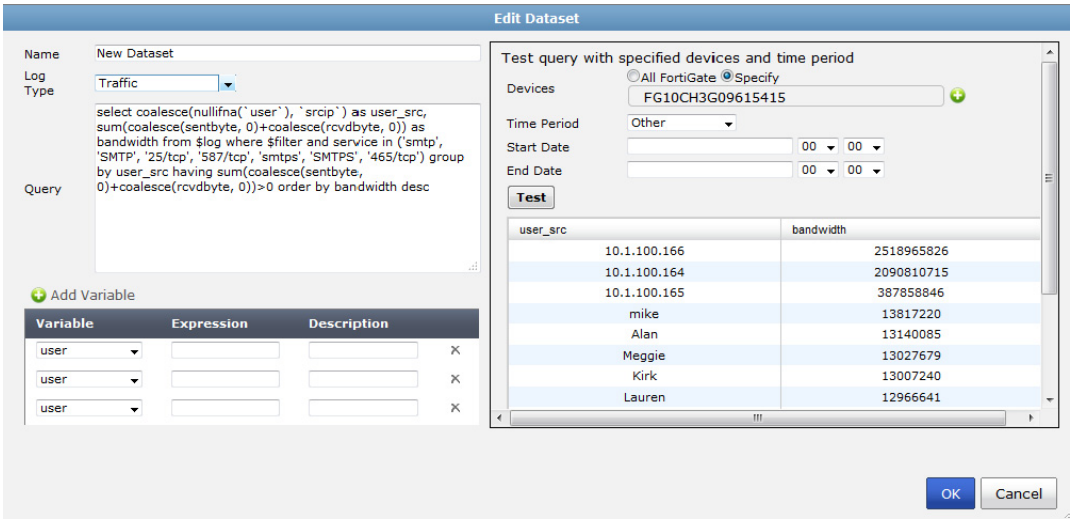
3. Edit the information as needed and test the query to ensure that the dataset functions as expected.
4. Select *OK* to clone the dataset and create a new dataset.

To edit a dataset:

1. Go to the *Reports* tab and select *Advanced* > *Dataset* in the tree menu.
2. Double-click on the dataset that you would like to edit, or select the dataset and select *Edit* from the toolbar or right-click menu.

   The *Edit Dataset* dialog box opens.

Figure 281: Edit dataset dialog box



3. Edit the information as required and test the query to ensure that the dataset functions as expected.

4. Select *OK* to finish editing the dataset.

Predefined datasets cannot be edited, the information is read-only. You can view the SQL query and variables used in the dataset and test against specific devices or log arrays.

To delete datasets:

1. Go to the *Reports* tab and select *Advanced* > *Dataset* in the tree menu.
2. Select the dataset or datasets that you would like to delete and select *Delete* from the toolbar or right-click menu.

Predefined datasets cannot be deleted, the information is read-only.

3. Select *OK* in the confirmation dialog box to delete the datasets or datasets.

To view the SQL query for an existing dataset:

1. Go to the *Reports* tab and select *Advanced* > *Dataset* in the tree menu.
2. Hover the mouse cursor over one of the datasets in the list.
3. The SQL query is displayed in the pop-up window.

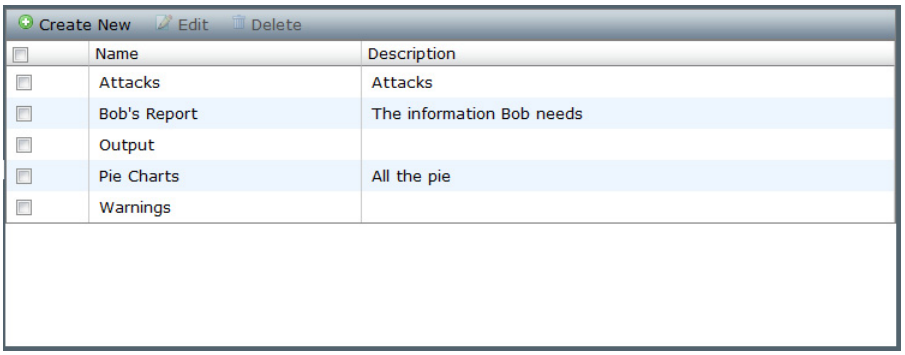
Figure 282:SQL query pop-up window



Output profile

Output profiles allow you to define email addresses to which generated reports are sent, and provides an option to upload the reports to FTP, SFTP, or SCP servers. Once created, an output profile can be specified in a report schedule; see “Schedules” on page 422.

Figure 283: Output profile page





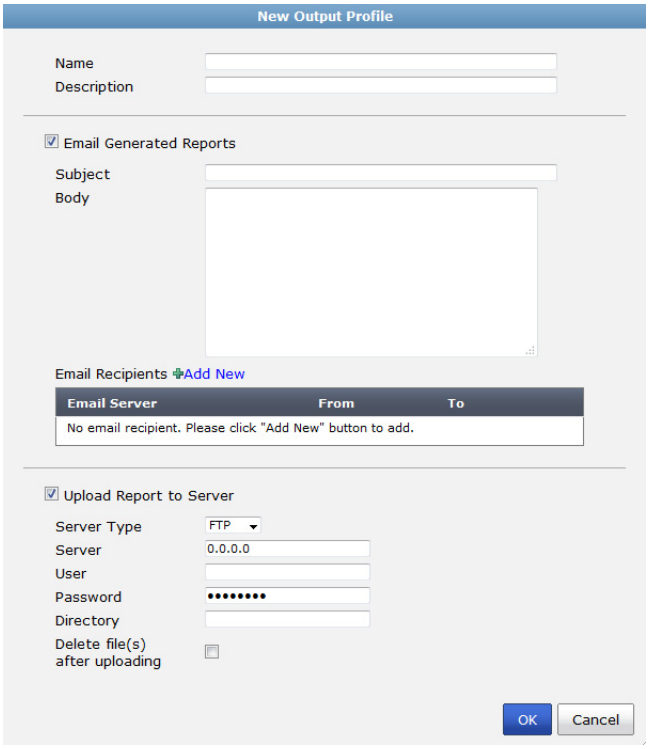
You must configure a mail server before you can configure an output profile.

To create a new output profile:

1. Go to the *Reports* tab and select *Advanced* > *Output Profile* in the tree menu.
2. Select *Create New* on the toolbar, or right-click in the output profile list and select *New* from the pop-up menu.

   The *Create New Output Profile* dialog box opens.

Figure 284: Create new output profile dialog box



3. Enter the following information:

Name	Enter a name for the new output profile.
Description	Enter a description for the output profile (optional).
Email Generated Reports	Enable email generated reports.
Subject	Enter a subject for the report email.
Body	Enter body text for the report email.
Email Recipients	Select the email server from the drop-down list and enter to and from email addresses. Select the plus (+) icon to add another entry so that you can specify multiple recipients.
Upload Report to Server	Enable uploading the reports to a server.
Server Type	Select *FTP, SFTP,* or *SCP* from the drop-down list.
Server	Enter the server IP address.
User	Enter the username.
Password	Enter the password.
Directory	Specify the directory where the report will be saved.
Delete file(s) after uploading	Select to delete the report after it has been uploaded to the selected.

4. Select *OK* to create the new output profile.

To edit an output profile:

1. Go to the *Reports* tab and select *Advanced* > *Output Profile* in the tree menu.
2. Double-click on the output profile that you would like to edit, or select the output profile and select *Edit* from the toolbar or right-click menu. The *Edit Output Profile* dialog box opens.
3. Edit the information as required and select *OK* to finish editing the output profile.

To delete output profiles:

1. Go to the *Reports* tab and select *Advanced* > *Output Profile* in the tree menu.
2. Select the output profile or profiles that you would like to delete and select *Delete* from the toolbar or right-click menu.
3. Select *OK* in the confirmation dialog box to delete the selected output profile or profiles.

Language

The language of the reports can be specified when creating a report schedule (see "Schedules" on page 422). New languages can be added, and the name and description of the languages can be changed. The predefined languages cannot be edited.

The available report languages can be viewed in the *Reports* tab under *Advanced* > *Language*.

Figure 285: Report language



The available pre-configured report languages include:

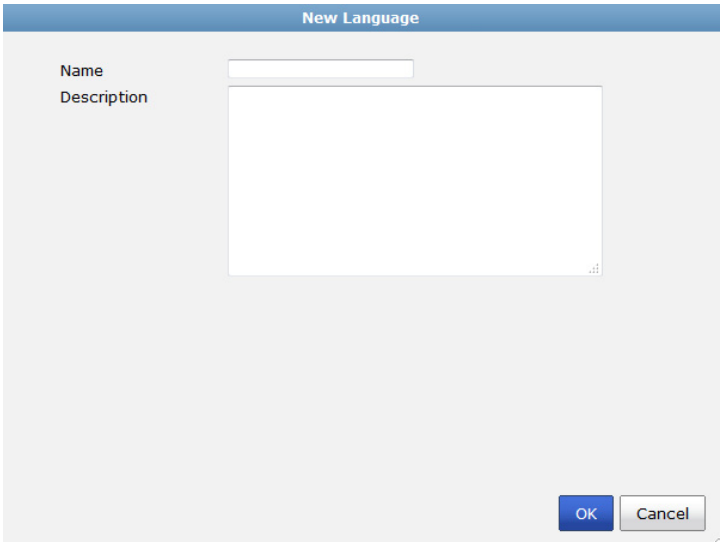
- English (default report language)
- French
- Japanese
- Korean
- Portuguese
- Simplified Chinese
- Spanish
- Traditional Chinese

To add a language:

1. Go to the *Reports* tab and select *Advanced* > *Language* in the tree menu.
2. Select *Create New* on the toolbar, or right-click in the language list and select *New* from the pop-up menu.

   The *Create New Language* dialog box opens.

Figure 286: Create a new language



3. Enter a name and description for the language in the requisite fields.
4. Select *OK* to add the language.

Adding a new language does not create that language. It only adds a placeholder for that language that contains the language name and description.

To edit a language:

1. Go to the *Reports* tab and select *Advanced* > *Language* in the tree menu.
2. Double-click on the language that you would like to edit, or select the language and select *Edit* from the toolbar or right-click menu. The *Edit Language* dialog box opens.
3. Edit the information as required and select *OK* to finish editing the language.

Predefined languages cannot be edited, information is read-only.

To delete languages:

1. Go to the *Reports* tab and select *Advanced* > *Language* in the tree menu.
2. Select the language or languages that you would like to delete and select *Delete* from the toolbar or right-click menu.
3. Select *OK* in the confirmation dialog box to delete the selected language or languages.

Predefined languages cannot be deleted, information is read-only.

FortiGuard Management

The FortiGuard Distribution Network (FDN) provides FortiGuard services for your FortiManager system and its managed devices and FortiClient agents. The FDN is a world-wide network of FortiGuard Distribution Servers (FDS) which update the FortiGuard services on your FortiManager system on a regular basis so that your FortiManager system is protected against the latest threats.

The FortiGuard services available on the FortiManager system include:

- Antivirus and IPS engines and signatures
- Web filtering and email filtering rating databases and lookups (select systems)
- Vulnerability scan and management support for FortiAnalyzer

To view and configure these services, go to *FortiGuard* > *FortiGuard Management* > *Advanced Settings*.

In FortiGuard Management, you can configure the FortiManager system to act as a local FDS, or use a web proxy server to connect to the FDN. FortiManager systems acting as a local FDS synchronize their FortiGuard service update packages with the FDN, then provide FortiGuard these updates and look up replies to your private network's FortiGate devices. The local FDS provides a faster connection, reducing Internet connection load and the time required to apply frequent updates, such as antivirus signatures, to many devices.

As an example, you might enable FortiGuard services to FortiGate devices on the built-in FDS, then specify the FortiManager system's IP address as the override server on your devices. Instead of burdening your Internet connection with all the devices downloading antivirus updates separately, the FortiManager system would use the Internet connection once to download the FortiGate antivirus package update, then redistribute the package to the devices.

FortiGuard Management also includes firmware revision management. To view and configure firmware options, go to *FortiGuard Management* > *Firmware Images*. You can download these images from the Customer Service & Support portal to install on your managed devices or on the FortiManager system.

Before you can use your FortiManager system as a local FDS, you must:

- Register your devices with Fortinet Customer Service & Support and enable the FortiGuard service licenses. See your device documentation for more information on registering your products.
- If the FortiManager system's Unregistered Device Options do not allow service to unregistered devices, add your devices to the device list, or change the option to allow service to unregistered devices. For more information, see the *FortiManager v5.0 Patch Release 5 CLI Reference*.

  For information about FDN service connection attempt handling or adding devices, see "Device Manager" on page 129.
- Enable and configure the FortiManager system's built-in FDS. For more information, see "Configuring network interfaces" on page 87.
- Connect the FortiManager system to the FDN.

  The FortiManager system must retrieve service update packages from the FDN before it can redistribute them to devices and FortiClient agents on the device list. For more information, see "Connecting the built-in FDS to the FDN" on page 453.

- Configure each device or FortiClient endpoint to use the FortiManager system's built-in FDS as their override server. You can do this when adding a FortiGate system. For more information, see "Adding a device" on page 147.

This section contains the following topics:

- Advanced settings
- Configuring devices to use the built-in FDS
- Configuring FortiGuard services
- Logging events related to FortiGuard services
- Restoring the URL or antispam database
- Package management
- Query server management
- Firmware images



For information on current security threats, virus and spam sample submission, and FortiGuard service updates available through the FDN, including antivirus, IPS, web filtering, and email filtering, see the FortiGuard Center web site, http://www.fortiguard.com/.

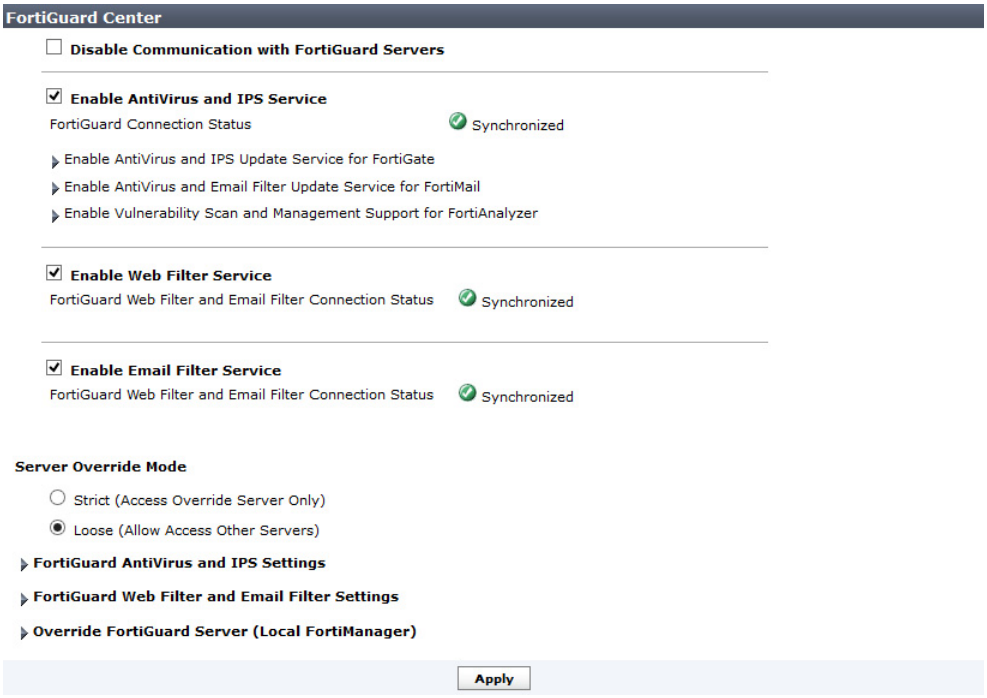
Advanced settings

The advanced settings provides a central location for configuring and enabling your FortiManager system's built-in FDS as an FDN override server.

By default, this option is disabled and devices contact FDN directly. After enabling and configuring FortiGuard, and configuring your devices to use the FortiManager system as their FortiGuard server, you can view overall and per device statistics on FortiGuard service benefits. FortiGuard Management has three supported configuration options:

- Antivirus and IPS Update Service for FortiGate
- Antivirus and email filter update Service for FortiMail
- Vulnerability Scan and Management Support for FortiAnalyzer

Figure 287: FortiGuard Center advanced settings



Configure the following settings:

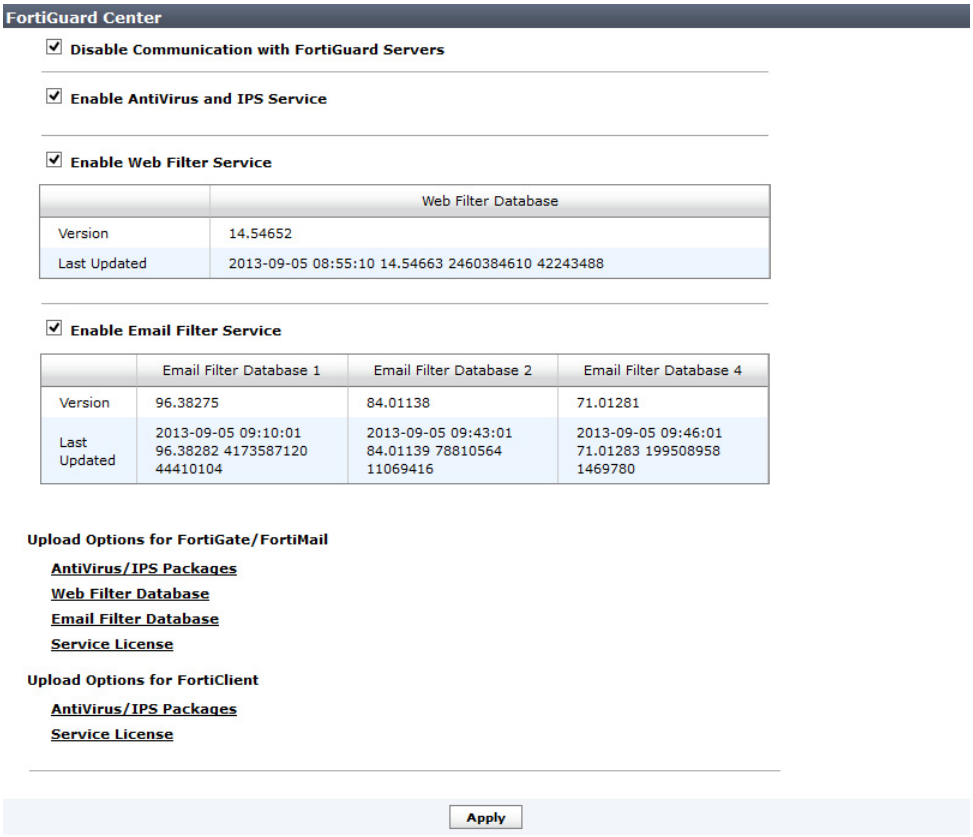
Disable Communication with FortiGuard Servers	Disable communication with the FortiGuard servers.
Enable Antivirus and IPS Service	Select to enable antivirus and intrusion protection service.
FortiGuard Connection Status	The status of the current connection between the FDN and the FortiManager system. • Disconnected: A red down arrow appears when the FDN connection fails. • Connected: A green up arrow appears when the initial FDN connection succeeds, but a synchronization connection has not yet occurred. • Out of Sync: A gray X appears when the initial FDN connection succeeds, but the built-in FDS is disabled. • Synchronized: A green checkmark appears when the built-in FDS is enabled, and the FDN packages download successfully.
Enable Antivirus and IPS Update Service for FortiGate	Select the OS versions from the table for updating antivirus and intrusion protection for FortiGate. You can select to download updates for FortiOS versions 5.0, 4.0, and 3.0.
Enable Antivirus and Email Filter Update Service for FortiMail	Select the OS versions from the table for updating antivirus and email filter for FortiMail. You can select to download updates for FortiMail OS versions 4.0 and 3.0.

Enable Vulnerability Scan and Management Support for FortiAnalyzer	Select the OS versions from the table for supporting Vulnerability Scan and Management Support for FortiAnalyzer. You can select to download updates for FortiAnalyzer OS versions 5.0 and 4.0.
Enable Web Filter and Services	Select to enable web filter services.
FortiGuard Web Filter and Email Filter Connection Status	The status of the current connection between the FDN and the FortiManager system. See FortiGuard Connection Status for more information.
Enable Email Filter Services	Select to enable email filter services.
FortiGuard Web Filter and Email Filter Connection Status	The status of the current connection between the FDN and the FortiManager system. See FortiGuard Connection Status for more information.
Server Override Mode	Select *Strict (Access Override Server Only)* or *Loose (Allow Access Other Servers)* override mode.
FortiGuard Antivirus and IPS Settings	
FortiGuard Distribution Network (FDN)	Select the required settings from the following options: • *Use Override Service Address for FortiGate/FortiMail:* enter an IP address and port number. Select the plus (+) icon to add multiple override server addresses (maximum = 10). • *Allow Push Update*: enter an IP address and port if selected • *Use Web Proxy*: enter an IP address, port, user name, and password is selected • *Schedule Regular Updates*: enter the update frequency from the drop-down lists if selected. Click *Update* to apply the changes.
Advanced	Select whether or not *Update Entries from FDS Server* and *Update Histories for Each FortiGate* are logged.
FortiGuard Web Filter and Email Filter Settings	
Connection to FDS Server(s)	Select the required settings from the following options: • *Use Override Server Address for FortiClient*: enter an IP address and port number. Select the plus (+) icon to add multiple override server addresses (maximum = 10). • *Use Override Server Address for FortiGate/FortiMail*: enter an IP address and port number. Select the plus (+) icon to add multiple override server addresses (maximum = 10). • *Use Web Proxy*: Enter an IP address, port, user name, and password if selected. • *Polling Frequency*: Enter the polling frequency from the drop-down lists. Click *Update* to apply the changes.

Log Settings	Select the required settings from the following options: • *Log FortiGuard Server Update Events*: enable or disable • *FortiGuard Web Filtering*: Choose from *Log URL disabled*, *Log non-url events*, *Log all URL lookups.* • *FortiGuard Anti-spam*: Choose from *Log Spam disabled*, *Log non-spam events*, *Log all Spam lookups.* • *FortiGuard Anti-virus Query*: Choose from *Log Virus disabled*, *Log non-virus events*, *Log all Virus lookups*.
Override FortiGuard Server (Local FortiManager)	
Additional Number of Private FortiGuard Servers	Select the plus (+) icon on the right side of the column to add additional private servers. Enter the IP address and selected the time zone of the private server to be added.
Enable Antivirus and IPS Update Service for Private Server	Select to enable antivirus and IPS update service for private servers.
Enable Web Filter and Email Filter Update Service for Private Server	Select to enable web filter and email filter update service for private servers.
Allow FortiGates to Access Public FortiGuard Servers when Private Servers are Unavailable	Select to allow FortiGates to access public FortiGuard servers when private serves are unavailable.

When selecting to disable communication with FortiGuard servers, you must manually upload packages for FortiGate, FortiMail, and FortiClient.

Figure 288: FortiGuard Center advanced settings (FortiGuard server communication disabled)



The following options are available:

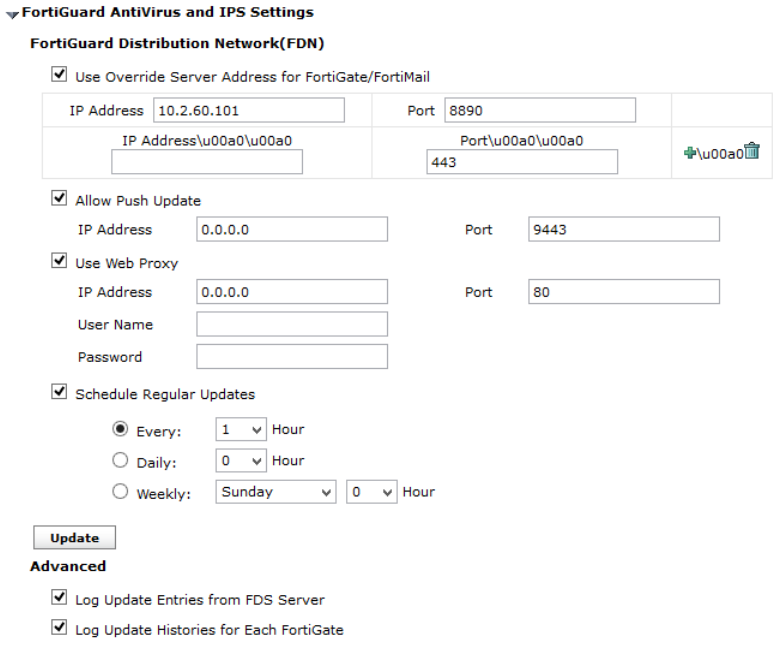
Disable Communication with FortiGuard Servers	Select to disable communication with the FortiGuard servers. When this option is selected, you must manually upload packages for FortiGate, FortiMail, and FortiClient.
Enable Antivirus and IPS Service	Select to enable antivirus and intrusion protection service.
Enable Web Filter Services	Select to enable web filter services. The Web Filter database is displayed.
Enable Email Filter Services	Select to enable email filter services. The Email Filter database is displayed.
Upload Options for FortiGate/FortiMail	
AntiVirus/IPS Packages	Select to upload the FortiGate/FortiMail antivirus and IPS packages. Browse for the file you downloaded from the Customer Service & Support portal on your management computer. Select *OK* to upload the package to FortiManager.
Web Filter Database	Select to upload the web filter database. Browse for the file you downloaded from the Customer Service & Support portal on your management computer. Select *OK* to upload the package to FortiManager.

Email Filter Database	Select to upload the email filter database. Browse for the file you downloaded from the Customer Service & Support portal on your management computer. Select *OK* to upload the package to FortiManager.
Service License	Select to import the FortiGate license. Browse for the file on your management computer. Select *OK* to upload the package to FortiManager.
Upload Options for FortiClient	
AntiVirus/IPS Packages	Select to upload the FortiClient AntiVirus/IPS packages. Browse for the file you downloaded from the Customer Service & Support portal on your management computer. Select *OK* to upload the package to FortiManager.
Service License	Select to import the FortiClient license. Browse for the file on your management computer. Select *OK* to upload the package to FortiManager.

FortiGuard antivirus and IPS settings

In this section you can enable settings for FortiGuard Antivirus and IPS settings.

Figure 289: FortiGuard antivirus and IPS settings



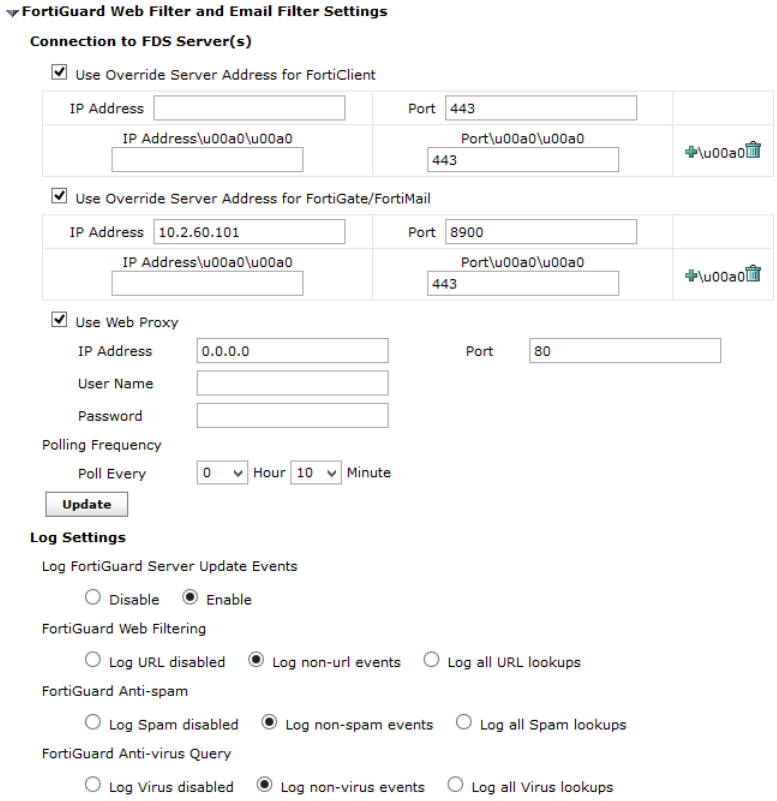
Configure the following settings:

Use Override Server Address for FortiGate/FortiMail	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the plus (+) icon to add additional override servers. To override the default server for updating FortiGate/FortiMail device's FortiGuard services, see "Overriding default IP addresses and ports" on page 457.
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 456.
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 456.
Scheduled Regular Updates	Configure when packages are updated without manually initiating an update request. To schedule regular service updates, see "Scheduling updates" on page 458.
Update	Select to immediately update the configured antivirus and email filter settings.
Advanced	Enables logging of service updates and entries. If either check box is not selected, you will not be able to view these entries and events when you select *View FDS and FortiGuard Download History*.

FortiGuard web and email filter settings

In this section you can enable settings for FortiGuard Web Filter and Email Filter.

Figure 290: FortiGuard web filter and email filter settings



Configure the following settings:

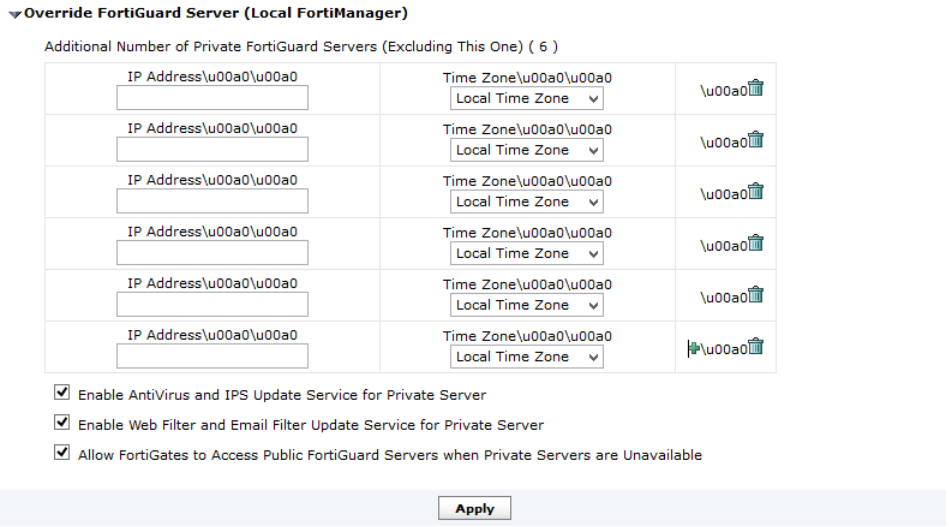
Connection to FDS server(s)	Configure connections for overriding the default built-in FDS or web proxy server for web filter and email filter settings. To override an FDS server for web filter and email filter services, see "Overriding default IP addresses and ports" on page 457. To enable web filter and email filter service updates using a web proxy server, see "Enabling updates through a web proxy" on page 456.
Use Override Server Address for FortiClient	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the plus (+) icon to add additional override servers.
Use Override Server Address for FortiGate/FortiMail	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the plus (+) icon to add additional override servers. To override the default server for updating FortiGate device's FortiGuard services, see "Overriding default IP addresses and ports" on page 457.

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 456.
Log Settings	Configure logging of FortiGuard web filtering, email filter, and antivirus query events. To configure logging of FortiGuard web filtering and email filtering events, see "Logging FortiGuard web or email filter events" on page 460

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.

Figure 291: Override FortiGuard server



Configure the following settings:

Additional number of private FortiGuard servers (excluding this one) (1) +	Select the plus (+) icon to add a private FortiGuard server. When adding a private server, you must enter its IP address and time zone.
Enable Antivirus and IPS Update Service for Private Server	When one or more private FortiGuard servers are configured, update antivirus and IPS through this private server instead of using the default FDN. This option is available only when a private server has been configured.

Enable Web Filter and Email Filter Update Service for Private Server	When one or more private FortiGuard servers are configured, update the web filter and email filter through this private server instead of using the default FDN. This option is available only when a private server has been configured.
Allow FortiGates to access public FortiGuard servers when private servers unavailable	When one or more private FortiGuard servers are configured, managed FortiGate units will go to those private servers for FortiGuard updates. Enable this feature to allow those FortiGate units to then try to access the public FDN servers if the private servers are unreachable. This option is available only when a private server has been configured.



The FortiManager system's network interface settings can restrict which network interfaces provide FDN services. For more information, see "Configuring network interfaces" on page 87.

Connecting the built-in FDS to the FDN

When you enable the built-in FDS and initiate an update either manually or by a schedule, the FortiManager system attempts to connect to the FDN.

If all connection attempts to the server list fail, the connection status will be *Disconnected*.

If the connection status remains *Disconnected*, you may need to configure the FortiManager system's connection to the FDN by:

- overriding the default IP address and/or port
- configuring a connection through a web proxy

After establishing a connection with the FDN, the built-in FDS can receive FortiGuard service update packages, such as antivirus engines and signatures or web filtering database updates, from the FDN.

To enable the built-in FDS:

1. Go to *FortiGuard Management* > *Advanced Settings*.
2. Enable the types of FDN services that you want to provide through your FortiManager system's built-in FDS.

   For more information, see "Configuring FortiGuard services" on page 455.
3. Select *Apply*.

   The built-in FDS attempts to connect to the FDN. To see the connection status go to *FortiGuard Management* > *Advanced Settings*.

Disconnected	A red down arrow appears when the FDN connection fails.
Connected	A green up arrow appears when the initial FDN connection succeeds, but a synchronization connection has not yet occurred.

Out Of Sync	A gray X appears when the initial FDN connection succeeds, but the built-in FDS is disabled, and so cannot synchronize.
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 87.



If you still cannot connect to the FDN, check routes, DNS, and any intermediary firewalls or NAT devices for policies that block necessary FDN ports and protocols. For additional FDN troubleshooting information, including FDN server selection, "FDN port numbers and protocols" on page 457 and the Knowledge Base article FortiGuard Distribution Network: Accessing and Debugging FortiGuard Services.

Configuring devices to use the built-in FDS

After enabling and configuring the FortiManager system's built-in FDS, you can configure devices to use the built-in FDS by providing the FortiManager system's IP address and configured port as their override server.

Devices are not required to be registered with FortiManager system's *Device Manager* to use the built-in FDS for FortiGuard updates and services.

Procedures for configuring devices to use the built-in FDS vary by device type. See the documentation for your device for more information.



If you are connecting a device to a FortiManager system's built-in FDS, some types of updates, such as antivirus engine updates, require you to enable SSH and HTTPS Administrative Access on the network interface which will receive push updates. If the settings are disabled, see "Network" on page 85.

Matching port settings

When configuring a device to override default FDN ports and IP addresses with that of a FortiManager system, the default port settings for the device's update or query requests may not match the listening port of the FortiManager system's built-in FDS. If this is the case, the device's requests will fail. To successfully connect them, you must match the devices' port settings with the FortiManager system's built-in FDS listening ports.

For example, the default port for FortiGuard antivirus and IPS update requests is TCP 443 on FortiOS v4.0 and higher, but the FortiManager system's built-in FDS listens for those requests on TCP 8890. In this case, the FortiGate unit's update requests would fail until you configure the unit to send requests on TCP 8890.

In some cases, the device may not be configurable; instead, you must configure the FortiManager system to listen on an alternate port.

Handling connection attempts from unregistered devices

The built-in FDS replies to FortiGuard update and query connections from devices registered with the device manager's device list. If the FortiManager is configured to allow connections from unregistered devices, unregistered devices can also connect.

For example, you might choose to manage a FortiGate unit's firmware and configuration locally (from its Web-based Manager), but use the FortiManager system when the FortiGate unit requests FortiGuard antivirus and IPS updates. In this case, the FortiManager system considers the FortiGate unit to be an unregistered device, and must decide how to handle the connection attempt. The FortiManager system will handle the connection attempt based on how it is configured. Connection attempt handling is only configurable via the CLI

To configure connection attempt handling:

1. Go to the CLI console widget in the *System Settings* tab. For information on widget settings, see "Customizing the dashboard" on page 60.
2. Click inside the console to connect.
3. Enter the following CLI command to allow unregistered devices to be registered:

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

4. To configure the system to add unregistered devices and allow service requests, enter the following CLI commands:

```
config system admin setting
  set unreg_dev_opt add_allow_service
end
```

5. To configure the system to add unregistered devices but deny service requests, enter the following CLI commands:

```
config system admin setting
  set unreg_dev_opt add_no_service
end
```

For more information, see the *FortiManager CLI Reference*.

Configuring FortiGuard services

The FortiGuard Management provides a central location for configuring how the FortiManager system accesses the FDN and FDS, including push updates. The following procedures explain how to configure FortiGuard services and configuring override and web proxy servers, if applicable.

If you need to host a custom URL list that are rated by the FortiGate unit, you can import a list using the CLI.

Enabling push updates

When an urgent or critical FortiGuard antivirus or IPS signature update becomes available, the FDN can push update notifications to the FortiManager system's built-in FDS. The FortiManager system then immediately downloads the update.

To use push update, you must enable both the built-in FDS and push updates. Push update notifications will be ignored if the FortiManager system is not configured to receive them. If TCP port 443 downloads must occur through a web proxy, you must also configure the web proxy connection. See "Enabling updates through a web proxy" on page 456.

If push updates must occur through a firewall or NAT device, you may also need to override the default push IP address and port.

For example, overriding the push IP address can be useful when the FortiManager system has a private IP address, and push connections to a FortiManager system must traverse NAT. Normally, when push updates are enabled, the FortiManager system sends its IP address to the FDN; this IP address is used by the FDN as the destination for push messages; however, if the FortiManager system is on a private network, this IP address may be a private IP address, which is not routable from the FDN – causing push updates to fail.

To enable push through NAT, enter a push IP address override, replacing the default IP address with an IP address of your choice such as the NAT device's external or virtual IP address. This causes the FDN to send push packets to the override IP address, rather than the FortiManager system's private IP address. The NAT device can then forward the connection to the FortiManager system's private IP address.



The built-in FDS may not receive push updates if the external IP address of any intermediary NAT device is dynamic (such as an IP address from PPPoE or DHCP). When the NAT device's external IP address changes, the FortiManager system's push IP address configuration becomes out-of-date.

To enable push updates to the FortiManager system:

1. Go to *FortiGuard Management* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*; see Figure 289 on page 449.
3. Select the check box beside *Allow Push Update*.
4. If there is a NAT device or firewall between the FortiManager system and the FDN which denies push packets to the FortiManager system's IP address on UDP port 9443, enter the IP Address and/or Port number on the NAT device which will forward push packets to the FortiManager system. The FortiManager system will notify the FDN to send push updates to this IP address and port number.
   - *IP Address* is the external or virtual IP address on the NAT device for which you will configure a static NAT or port forwarding.
   - *Port* is the external port on the NAT device for which you will configure port forwarding.
5. Select *Apply*.
6. If you performed step 4, also configure the device to direct that IP address and/or port to the FortiManager system.
   - If you entered a virtual IP address, configure the virtual IP address and port forwarding, and use static NAT mapping.
   - If you entered a port number, configure port forwarding; the destination port must be UDP port 9443, the FortiManager system's listening port for updates.

Enabling updates through a web proxy

If the FortiManager system's built-in FDS must connect to the FDN through a web (HTTP or HTTPS) proxy, you can specify the IP address and port of the proxy server.

If the proxy requires authentication, you can also specify a user name and password.

To enable updates to the FortiManager system through a proxy:

1. Go to *FortiGuard Management* > *Advanced Settings*.

2. If configuring a web proxy server to enable web and email filtering updates, expand *FortiGuard Web Filter and Email Filter Settings.*

   If configuring a web proxy to enable antivirus and IPS updates, expand *FortiGuard Antivirus and IPS Settings*; Figure 289 on page 449.
3. Select the check box beside *Use Web Proxy* and enter the IP address and port number of the proxy.
4. If the proxy requires authentication, enter the user name and password.
5. Select *Update* to immediately connect and receive updates from the FDN.

   The FortiManager system connects to the override server and receives updates from the FDN.
6. Select *Apply*.

If the FDN connection status is *Disconnected*, the FortiManager system is unable to connect through the web proxy.

Overriding default IP addresses and ports

FortiManager systems' built-in FDS connect to the FDN servers using default IP addresses and ports. You can override these defaults if you want to use a port or specific FDN server that is different from the default.

To override default IP addresses and ports:

1. Go to *FortiGuard Management* > *Advanced Settings*.
2. If you want to override the default IP address or port for synchronizing with available FortiGuard antivirus and IPS updates, select the arrow to expand *FortiGuard Antivirus and IPS Settings*, then select the check box beside *Use Override Server Address for FortiGate/FortiMail* and enter the IP address and/or port number for all FortiGate units.
3. Select *Update* to immediately connect and receive updates from the FDN.

   The FortiManager system connects to the override server and receives updates from the FDN.
4. If you want to override the FortiManager system's default IP address or port for synchronizing with available FortiGuard web and email filtering updates, select the arrow to expand *FortiGuard Web Filter and Email Filter Settings*.

   Select the appropriate check box beside *Use Override Server Address for FortiGate/FortiMail* and/or *Use Override Server Address for FortiClient* and enter the IP address and/or port number.
5. Select *Apply*.

If the FDN connection status remains disconnected, the FortiManager system is unable to connect with the configured override.

FDN port numbers and protocols

Both the built-in FDS and devices use certain protocols and ports to successfully request and receive updates from the FDN or override server. Any intermediary proxies or firewalls must allow these protocols and ports, or the connection will fail.

For troubleshooting information and details on FDN ports, see the *FortiManager v5.0 Patch Release 5 Release Notes* and the Knowledge Base article FDN Services and Ports.

After connecting to the FDS, you can verify connection status on the FortiGuard Management page. For more information about connection status, see "Connecting the built-in FDS to the FDN" on page 453.

Scheduling updates

Keeping the built-in FDS up-to-date is important to provide current FortiGuard update packages and rating lookups to requesting devices. This is especially true as new viruses, malware, and spam sources pop up on a very frequent basis. By configuring a scheduled update, you are guaranteed to have a relatively recent version of database updates.

A FortiManager system acting as an FDS synchronizes its local copies of FortiGuard update packages with the FDN when:

- you manually initiate an update request by selecting *Update Now*
- it is scheduled to poll or update its local copies of update packages
- if push updates are enabled, it receives an update notification from the FDN

If the network is interrupted when the FortiManager system is downloading a large file, it downloads all files again when the network resumes.

To schedule antivirus and IPS updates:

1. Go to *FortiGuard Management* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*; Figure 289 on page 449.
3. Select the check box beside *Schedule Regular Updates*.
4. Specify an hourly, daily, or weekly schedule.
5. Select *Apply*.

To schedule Web Filtering and Email Filter polling:

1. Go to *FortiGuard Management* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Web Filter and Email Filter Settings*.
3. In *Polling Frequency*, select the number of hours and minutes of the polling interval.
4. Select *Apply*.

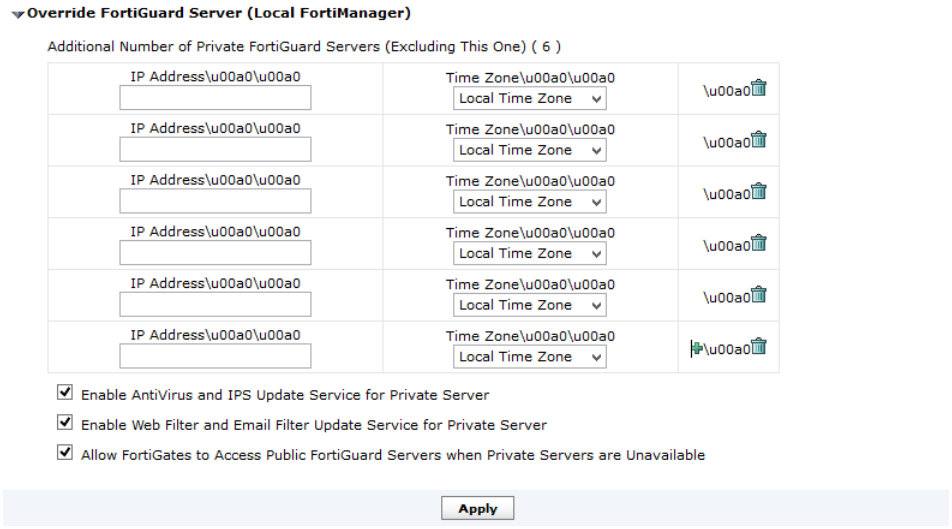


If you have formatted your FortiManager system's hard disk, polling and lookups will fail until you restore the URL and email filter databases. For more information, see "Restoring the URL or antispam database" on page 461.

Accessing public FortiGuard web and email filter servers

You can configure the FortiManager system to allow the managed FortiGate units to access public FortiGuard web filter or email filter network servers in the event local FortiGuard web filter or email filter server URL lookups fail. You can specify private servers where the FortiGate units can send URL queries.

Figure 292: Overriding FortiGuard Server



To access public FortiGuard web and email filter servers:

1. Go to *FortiGuard Management* > *Advanced Settings*.
2. Expand *Override FortiGuard Server (Local FortiManager)*.
3. Select the *Plus* (+) sign next to *Additional number of private FortiGuard servers (excluding this one) (0)*.
4. Enter the *IP Address* for the server, and select its *Time Zone*.
5. Repeat step 4 as often as required. You can include up to ten additional servers.
6. Select the additional options to set where the FDS updates come from, and if the managed FortiGate units can access these servers if the local FDS is not available.
   - Check the *Enable Antivirus and IPS update Service for Private Server* if you want the FDS updates to come from a private server.
   - Check the *Enable Web Filter and Email Filter Service for Private Server* if you want the updates to come from a private server.
   - Click *Allow FortiGates to access public FortiGuard servers when private servers unavailable* if you want to the updates to come from public servers in case the private servers are unavailable.
7. Select *Apply*.

Logging events related to FortiGuard services

You can log a variety of events related to FortiGuard services.



Logging events from the FortiManager system's built-in FDS requires that you also enable local event logging.

Logging FortiGuard antivirus and IPS updates

You can track FortiGuard antivirus and IPS updates to both the FortiManager system's built-in FDS and any registered FortiGate devices which use the FortiManager system's FDS.

To log updates and histories to the built-in FDS:

1. Go to *FortiGuard Management* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*; see Figure 289 on page 449.
3. Under the *Advanced* heading, enable *Log Update Entries from FDS Server*.
4. Select *Apply*.

To log updates to FortiGate devices:

1. Go to *FortiGuard Management* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Antivirus and IPS Settings*; see Figure 289 on page 449.
3. Under the *Advanced* heading, enable *Log Update Histories for Each FortiGate*.
4. Select *Apply*.

Logging FortiGuard web or email filter events

You can track FortiGuard web filtering and email filtering lookup and non-events occurring on any registered FortiGate device which uses the FortiManager system's FDS.

Before you can view lookup and non-event records, you must enable logging for FortiGuard web filtering or email filter events.

To log rating queries:

1. Go to *FortiGuard Management* > *Advanced Settings*.
2. Select the arrow to expand *FortiGuard Web Filtering and Email Filter Settings*.
3. Select the log settings:

Log FortiGuard Server Update Events	Enable or disable logging of FortiGuard server update events.
FortiGuard Web Filtering	
Log URL disabled	Disable URL logging.
Log non-URL events	Logs only non-URL events.
Log all URL lookups	Logs all URL lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
FortiGuard Antispam	
Log Spam disabled	Disable spam logging.
Log non-spam events	Logs email rated as non-spam.
Log all Spam lookups	Logs all spam lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
FortiGuard Anti-virus Query	
Log Virus disabled	Disable virus logging.

Log non-virus events	Logs only non-virus events.
Log all Virus lookups	Logs all virus queries sent to the FortiManager system's built-in FDS by FortiGate devices.

4. Select *Apply*.

Restoring the URL or antispam database

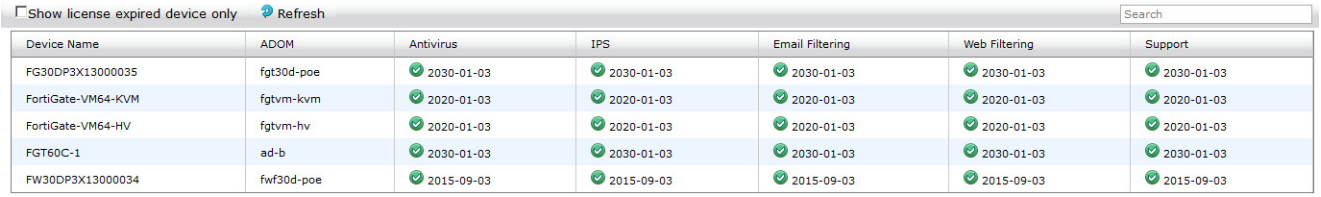
Formatting the hard disk or partition on FortiManager 3000 units and higher deletes the URL and antispam databases required to provide FortiGuard email filter and web filtering services through the built-in FDS. The databases will re-initialize when the built-in FDS is scheduled next, to synchronize them with the FDN.

Before formatting the hard disk or partition, you can back up the URL and antispam database using the CLI, which encrypts the file. You can also back up licenses as well. The databases can be restored by importing them using the CLI. If you have created a custom URL database, you can also backup or restore this customized database (for FortiGate units).

Licensing status

FortiManager includes a licensing overview page that allows you to view license information for all managed FortiGate devices. To view the licensing status, go to the *FortiGuard* tab and select *Licensing Status* in the tree menu.

Figure 293: Licensing status page



This page displays the following information:

Show license expired devices only	Select to display devices with an expired license only.
Refresh	Select the refresh icon to refresh the information displayed on this page.
Search	Use the search field to find a specific device in the table.
Device Name	The device name or hostname. You can change the order that devices are listed by clicking the column title.
ADOM	ADOM information. You can change the order that ADOMs are listed by clicking the column title.
Antivirus	The license status and expiration date. You can change the order that devices are listed by clicking the column title.

IPS	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Email Filtering	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Web Filtering	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Support	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Icon States	Green: License OK Orange: License will expire soon Red: License has expired

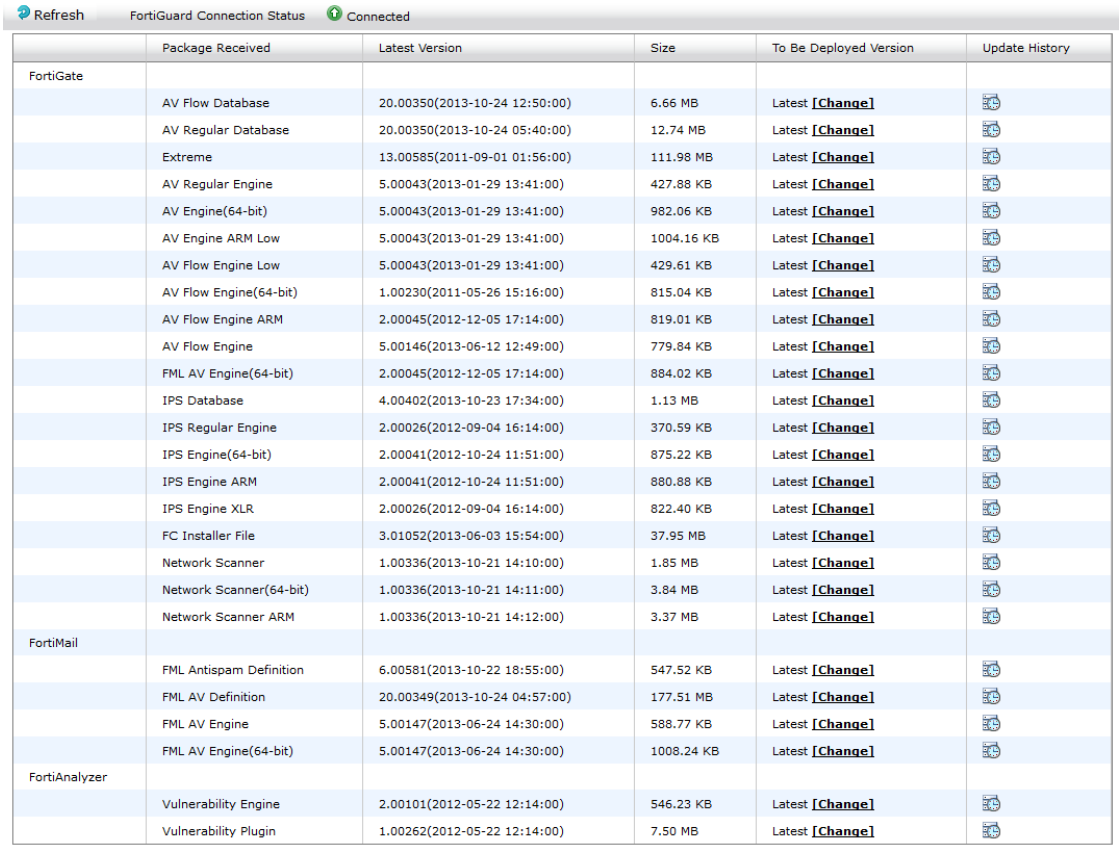
Package management

Antivirus and IPS signature packages are managed in *FortiGuard Management* > *Package Management*. Packages received from FortiGuard and the service status of managed devices are listed in *Receive Status* and *Service Status*, respectively.

Receive status

To view packages received from FortiGuard, go to *FortiGuard Management* > *Package Management* > *Receive Status*. This page displays the package received, version, size, to be deployed version, and update history or FortiGate, FortiMail, FortiAnalyzer, and FortiClient.

Figure 294: FortiGuard package receive status



	Package Received	Latest Version	Size	To Be Deployed Version	Update History
FortiGate					
	AV Flow Database	20.00350(2013-10-24 12:50:00)	6.66 MB	Latest [Change]	
	AV Regular Database	20.00350(2013-10-24 05:40:00)	12.74 MB	Latest [Change]	
	Extreme	13.00585(2011-09-01 01:56:00)	111.98 MB	Latest [Change]	
	AV Regular Engine	5.00043(2013-01-29 13:41:00)	427.88 KB	Latest [Change]	
	AV Engine(64-bit)	5.00043(2013-01-29 13:41:00)	982.06 KB	Latest [Change]	
	AV Engine ARM Low	5.00043(2013-01-29 13:41:00)	1004.16 KB	Latest [Change]	
	AV Flow Engine Low	5.00043(2013-01-29 13:41:00)	429.61 KB	Latest [Change]	
	AV Flow Engine(64-bit)	1.00230(2011-05-26 15:16:00)	815.04 KB	Latest [Change]	
	AV Flow Engine ARM	2.00045(2012-12-05 17:14:00)	819.01 KB	Latest [Change]	
	AV Flow Engine	5.00146(2013-06-12 12:49:00)	779.84 KB	Latest [Change]	
	FML AV Engine(64-bit)	2.00045(2012-12-05 17:14:00)	884.02 KB	Latest [Change]	
	IPS Database	4.00402(2013-10-23 17:34:00)	1.13 MB	Latest [Change]	
	IPS Regular Engine	2.00026(2012-09-04 16:14:00)	370.59 KB	Latest [Change]	
	IPS Engine(64-bit)	2.00041(2012-10-24 11:51:00)	875.22 KB	Latest [Change]	
	IPS Engine ARM	2.00041(2012-10-24 11:51:00)	880.88 KB	Latest [Change]	
	IPS Engine XLR	2.00026(2012-09-04 16:14:00)	822.40 KB	Latest [Change]	
	FC Installer File	3.01052(2013-06-03 15:54:00)	37.95 MB	Latest [Change]	
	Network Scanner	1.00336(2013-10-21 14:10:00)	1.85 MB	Latest [Change]	
	Network Scanner(64-bit)	1.00336(2013-10-21 14:11:00)	3.84 MB	Latest [Change]	
	Network Scanner ARM	1.00336(2013-10-21 14:12:00)	3.37 MB	Latest [Change]	
FortiMail					
	FML Antispam Definition	6.00581(2013-10-22 18:55:00)	547.52 KB	Latest [Change]	
	FML AV Definition	20.00349(2013-10-24 04:57:00)	177.51 MB	Latest [Change]	
	FML AV Engine	5.00147(2013-06-24 14:30:00)	588.77 KB	Latest [Change]	
	FML AV Engine(64-bit)	5.00147(2013-06-24 14:30:00)	1008.24 KB	Latest [Change]	
FortiAnalyzer					
	Vulnerability Engine	2.00101(2012-05-22 12:14:00)	546.23 KB	Latest [Change]	
	Vulnerability Plugin	1.00262(2012-05-22 12:14:00)	7.50 MB	Latest [Change]	

The following information is displayed:

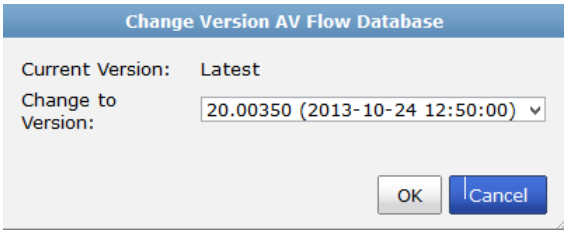
Refresh	Select to refresh the table.
FortiGuard Connection Status	The FortiGuard connection status.
	The device type: FortiGate, FortiMail, FortiAnalyzer, FortiClient.
Package Received	The name of the package.
Latest Version	The package version.
Size	The size of the package.
To Be Deployed Version	The package version that is to be deployed. Select Change to change the version. See “Deployed version” on page 463.
Update History	Select the icon to view the package update history. See “Update history” on page 464.

Deployed version

To change the to be deployed version of a received packaged, select *Change* in the *To Be Deployed Version* column for the package.

The *Change Version* dialog box opens, allowing you to select an available version from the drop-down list.

Figure 295: Change deployed package version

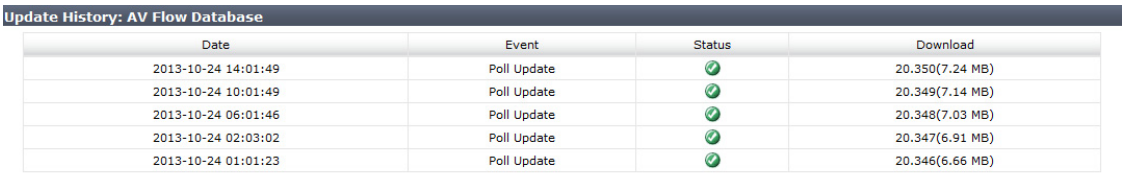


Update history

Selecting the update history button in a package's row will open the update history page for that package.

It shows the update times, the events that occurred, the statuses of the updates, and the versions downloaded.

Figure 296: Update history example (AV Flow Database)



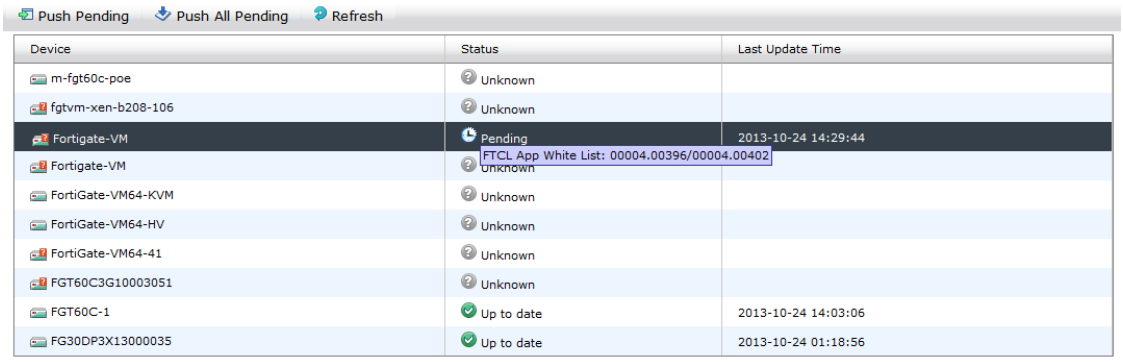
Service status

The service status page shows a list of all the managed FortiGate devices, their last update time, and their status. A device's status can be one of the following:

- Up to Date: the latest package has been received by the FortiGate unit.
- Pending: The FortiGate unit has an older version of the package due to an acceptable reason (such as the scheduled update time having not come yet).
- Problem: The FortiGate unit missed the scheduled query, or did not correctly receive the latest package.
- Unknown: The FortiGate unit's status is not currently known.

Pending updates can also be pushed to the devices, either individually or all at the same time. The list can be refreshed by selecting *Refresh* in the toolbar.

Figure 297: Package service status



This page displays the following:

Push Pending	Select the device in the list and select *Push Pending* in the toolbar to push the update to the device. This option is available in the right-click menu.
Push All Pending	Select *Push All Pending* in the toolbar to push the update to the devices in the list. This option is available in the right-click menu.
Refresh	Select to refresh the list.
Device	The device serial number or hostname is displayed.
Status	The service update status. Hover the mouse cursor over a pending icon to view the package to be installed.
Last Update Time	The date and time of the last update.

To push updates to a device or devices:

1. Go to *FortiGuard Management* > *Package Management* > *Service Status*.
2. Select *Push All Pending* in the toolbar, or right-click and select *Push All Pending* from the pop-up menu, to push all the pending packages to their devices.

   Select a device, then right-click and select *Push Pending* from the pop-up menu to push the pending package to that device.

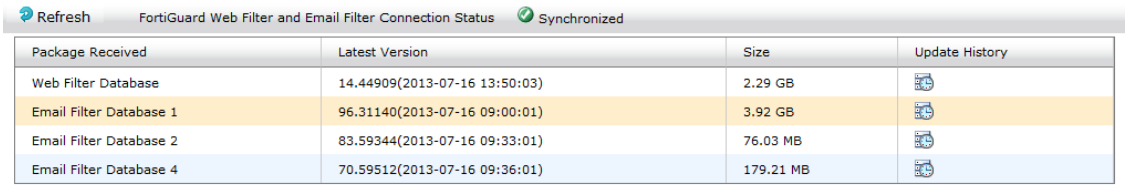
Query server management

The query server manager shows when updates are received from the server, the update version, the size of the update, and the update history. It also has graphs showing the number of queries from all the managed FortiGate units made to the FortiManager device.

Receive status

The view the received packages, go to *FortiGuard Management* > *Query Server Management* > *Receive Status*.

Figure 298: Query receive status



The following information is displayed:

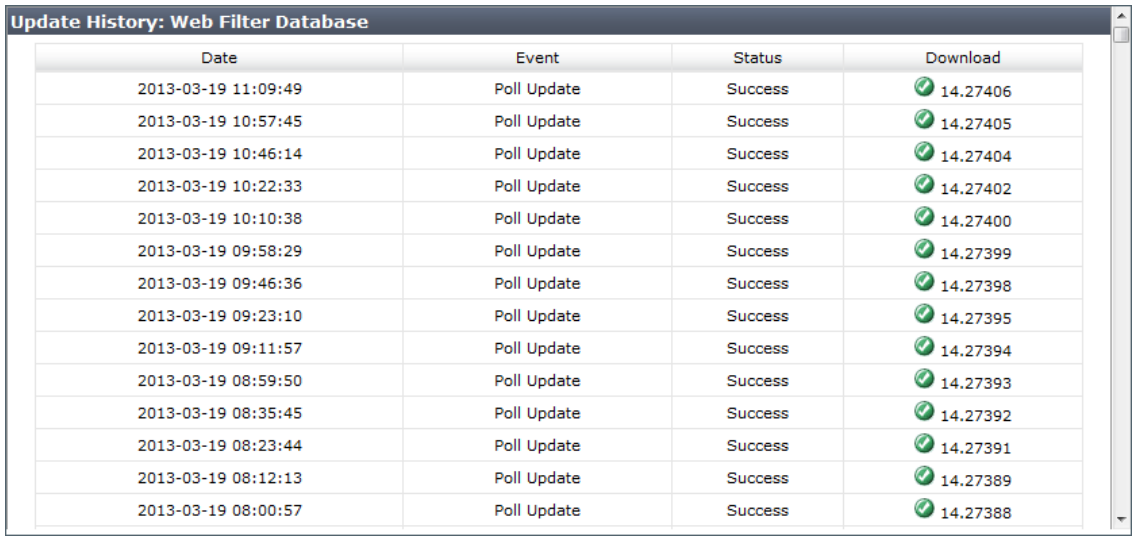
Refresh	Select to refresh the table.
Status	The *FortiGuard Web Filter and Email Filter Connection Status*.
Package Received	The name of the received package.

Latest Version	The latest version of the received package.
Size	The size of the package.
Update History	Select to view the package update history. See “Update history” on page 466.

Update history

Selecting the update history button for a package opens the update history page for that package.

Figure 299: Package update history



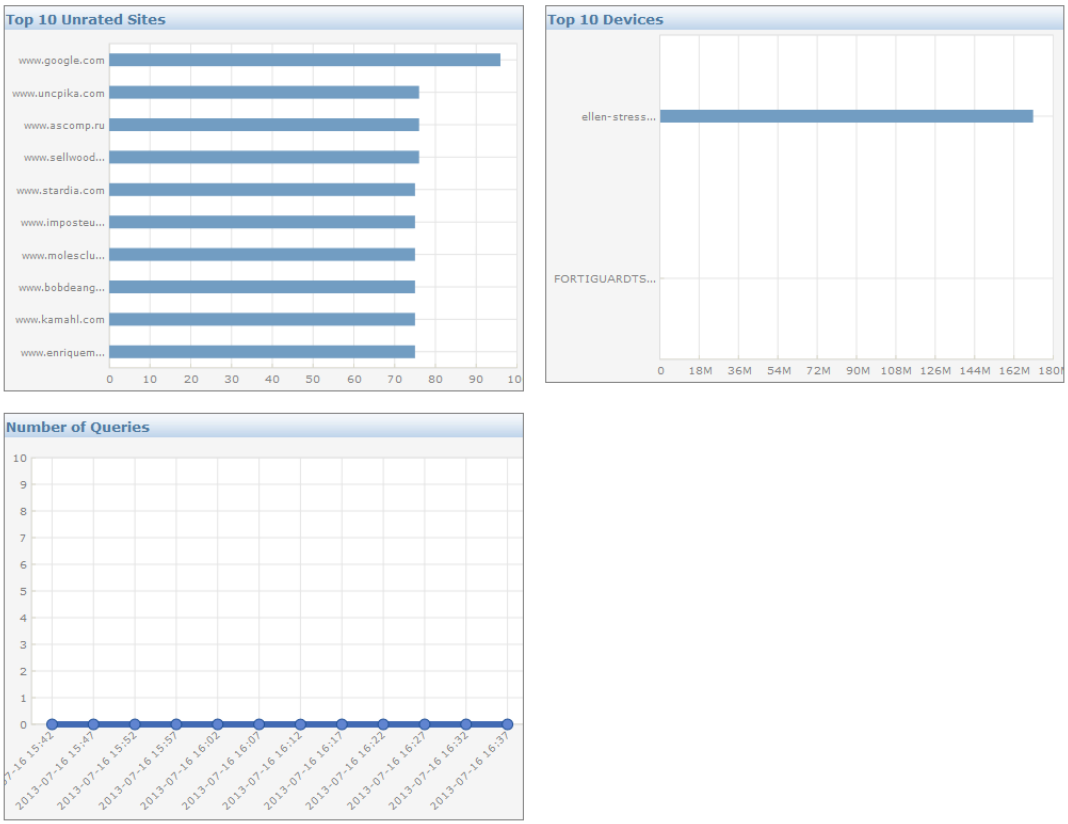
The following information is displayed:

Date	The date and time of the event.
Event	The event that occurred. One of: Manual Update or Poll Update.
Status	The status of the event.
Download	The version number and size of the download.

Query status

Go to *FortiGuard Management* > *Query Server Management* > *Query Status* to view graphs that show: the number of queries made from all managed devices to the FortiManager unit over a user selected time period, the top ten unrated sites, and the top ten devices for a user selected time period.

Figure 300: Query status example



The following information is displayed:

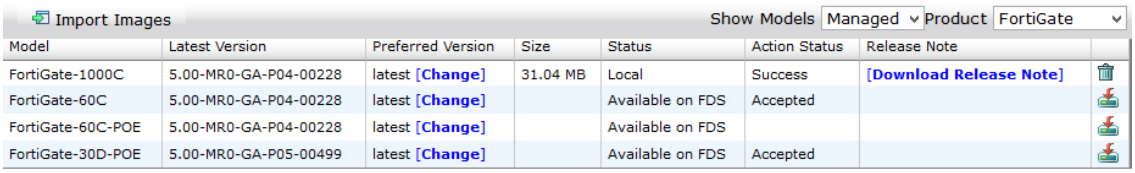
Top 10 Unrated Sites	Displays the top 10 unrated sites and the number of events. Select the refresh icon to refresh the graph information.
Top 10 Devices	Displays the top 10 devices and number of sessions. Select the edit icon to edit the statistics period. Select a time period from the drop-down list. Select the refresh icon to refresh the graph information.
Number of Queries	Displays the number of queries over a period of time. Select the edit icon to edit the statistics period. Select a time period from the drop-down list. Select the refresh icon to refresh the graph information.

Firmware images

Go to *FortiGuard Management* > *Firmware Images* to manage the firmware images stored on the FortiManager device. You can import firmware images for FortiGate, FortiCarrier, FortiAnalyzer, FortiManager, and FortiAP.

You can download only those images that are needed from the FDS systems, and customize which firmware images are available for deployment.

Figure 301: Firmware images list



The following information and settings are available:

Import Images	Select to open the firmware image import list. See "To import a firmware image:" on page 468.
Show Models	From the drop-down list, select *All* to show all the available models on the FortiGuard server, or select *Managed* to show only the models that are currently being managed by the FortiManager device.
Product	Select a managed product type from the drop-down list. Select one of *FortiGate, FortiCarrier, FortiAnalyzer, FortiManager,* or *FortiAP*.
Model	The device model number that the firmware is applicable to.
Latest Version	The latest version of the firmware that is available.
Preferred Version	The firmware version that you would like to use on the device. Select *Change* to open the *Change Version* dialog box, then select the desired version from the drop-down list and select *OK* to change the preferred version.
Size	The size of the firmware image.
Action Status	The status of the current action being taken.
Release Notes	A link to a copy of the release for the firmware image that has been downloaded.
Download/Delete	Download the firmware image from the FDS if it is available. If the firmware images has already been downloaded, then delete the firmware image from the FortiManager device.

For information about upgrading your FortiManager device, see "FortiManager Firmware" on page 479.

To import a firmware image:

1. Go to *FortiGuard Management* > *Firmware Images.* Select *Import Images* in the toolbar.

Figure 302: Firmware images import page



2. Select a device in the list and select Import in the toolbar.

   In the *Upload Firmware Image* dialog box, select *Browse* to browse to the desired firmware image file.

Figure 303: Local firmware images



3. Select *OK* to import the firmware image.

Firmware images can be downloaded from the Fortinet Customer Service & Support site at https://support.fortinet.com/ (support account required).

To delete firmware images:

1. Go to *FortiGuard Management* > *Firmware Images* and select *Import Images* in the toolbar.
2. Select the firmware images you would like to delete.
3. Select the *Delete* toolbar icon. A confirmation dialog box appears.
4. Select *OK* to delete the firmware images.

High Availability

This section provides a general description of FortiManager High Availability (HA). This section also describes all HA configuration options and includes some basic HA configuration and maintenance procedures.

This section describes:

- HA overview
- Configuring HA options
- Monitoring HA status
- Upgrading the FortiManager firmware for an operating cluster

HA overview

FortiManager high availability (HA) provides a solution for a key requirement of critical enterprise management and networking components: enhanced reliability. Understanding what's required for FortiManager reliability begins with understanding what normal FortiManager operations are and how to make sure that these normal operations continue if a FortiManager unit fails.

Most of the FortiManager operations involve storing FortiManager, and FortiGate configuration and related information in the FortiManager database on the FortiManager unit hard disk. A key way to enhance reliability of FortiManager is to protect the data in the FortiManager database from being lost if the FortiManager unit fails. This can be achieved by dynamically backing up FortiManager database changes to one or more backup FortiManager units. Then if the operating FortiManager unit fails, a backup FortiManager unit can take the place of the failed unit.

A FortiManager HA cluster consists of up five FortiManager units of the same FortiManager model. One of the FortiManager units in the cluster operates as a primary or master unit and the other one to four units operate as backup units. All of the units are visible on the network. The primary unit and the backup units can be at the same location. FortiManager HA also supports geographic redundancy so the primary unit and backup units can be in different locations attached to different networks as long as communication is possible between them (for example over the Internet, over a WAN, or through a private network).

Administrators connect to the primary unit Web-based Manager or CLI to perform FortiManager operations. Managed devices connect with the primary unit for configuration backup and restore. If FortiManager is used to distribute firmware updates and FortiGuard updates to managed devices, the managed devices can connect to the primary unit or one of the backup units.

If the primary FortiManager unit fails you must manually configure one of the backup units to become the primary unit. The new primary unit will have the same IP addresses as it did when it was the backup unit.



A reboot of the FortiManager device is not required when it is promoted from a slave to the master.

Synchronizing the FortiManager configuration and HA heartbeat

All changes to the FortiManager database are saved on the primary unit, and then these changes are synchronized to the backup units. The FortiManager configuration of the primary unit is also synchronized to the backup units (except for the HA parameters). Also, all firmware images and all FortiGuard data stored by the *Device Manager* are synchronized to the backup units. As a result, the backup units always match the primary unit. So if the primary unit fails, a backup unit can be configured to take the place of the primary unit and continue functioning as a standalone FortiManager unit.

While the FortiManager cluster is operating, all backup units in the cluster exchange HA heartbeat packets with the primary unit so that the primary unit can verify the status of the backup units and the backup units can verify the status of the primary unit. The HA heartbeat packets use TCP port 5199. HA heartbeat monitoring, as well as FortiManager database and configuration synchronization takes place using the connections between the FortiManager units in the cluster. As part of configuring the primary unit you add peer IPs and peer serial numbers of each of the backup FortiManager units in the cluster. You also add the peer IP of the primary unit and the primary unit serial number to each of the backup units.



Depending on the peer IPs that you use you can isolate HA traffic to specific FortiManager interfaces and connect those interfaces together so that they function as synchronization interfaces between the FortiManager units in the cluster. Communication between the units in the cluster must be maintained for the HA cluster to operate.

The interfaces used for HA heartbeat and synchronization communication can be connected to your network. However, if possible you should isolate HA heartbeat and synchronization packets from your network to save bandwidth.

If the primary unit or a backup unit fails

If the primary unit fails the backup units stop receiving HA heartbeat packets from the primary unit. If one of the backup units fails, the primary unit stops received HA heartbeat packets from the backup unit. In either case the cluster is considered down until it is reconfigured.

When the cluster goes down the cluster units still operating send SNMP traps and write log messages to alert the system administrator that a failure has occurred. You can also see the failure from the HA Status page.

You re-configure the cluster by removing the failed unit from the cluster configuration. If the primary unit has failed, this means configuring one of the backup units to be the primary unit and adding peer IPs for all of the remaining backup units to the new primary unit configuration.

If a backup unit has failed, you re-configure the cluster by removing the peer IP of the failed backup unit from the primary unit configuration.

Once the cluster is re-configured it will continue to operate as before but with fewer cluster units. If the failed unit is restored you can re-configure the cluster again to add the failed unit back into the cluster. In the same way you can add a new unit to the cluster by changing the cluster configuration to add it.

FortiManager HA cluster startup steps

FortiManager units configured for HA start up begin sending HA heartbeat packets to their configured peer IP addresses and also begin listening for HA heartbeat packets from their configured peer IP addresses.

When the FortiManager units receive HA heartbeat packets with a matching HA cluster ID and password from another from a peer IP address the FortiManager unit assumes the peer is functioning.

When the primary unit is receiving HA heartbeat packets from all of the configured peers or backup units, the primary unit sets the cluster status to up. Once the cluster is up the primary unit then synchronizes its configuration to the backup unit. This synchronization process can take a few minutes depending on the size of the FortiManager database. During this time database and configuration changes made to the primary unit are not synchronized to the backup units. Once synchronization is complete, if changes were made during synchronization, they are re-synchronized to the backup units.

Most of the primary unit configuration, as well as the entire FortiManager database, are synchronized to the backup unit. Interface settings and HA settings are not synchronized. These settings must be configured on each cluster unit.

Once the synchronization is complete, the FortiManager HA cluster begins normal operation.

Configuring HA options

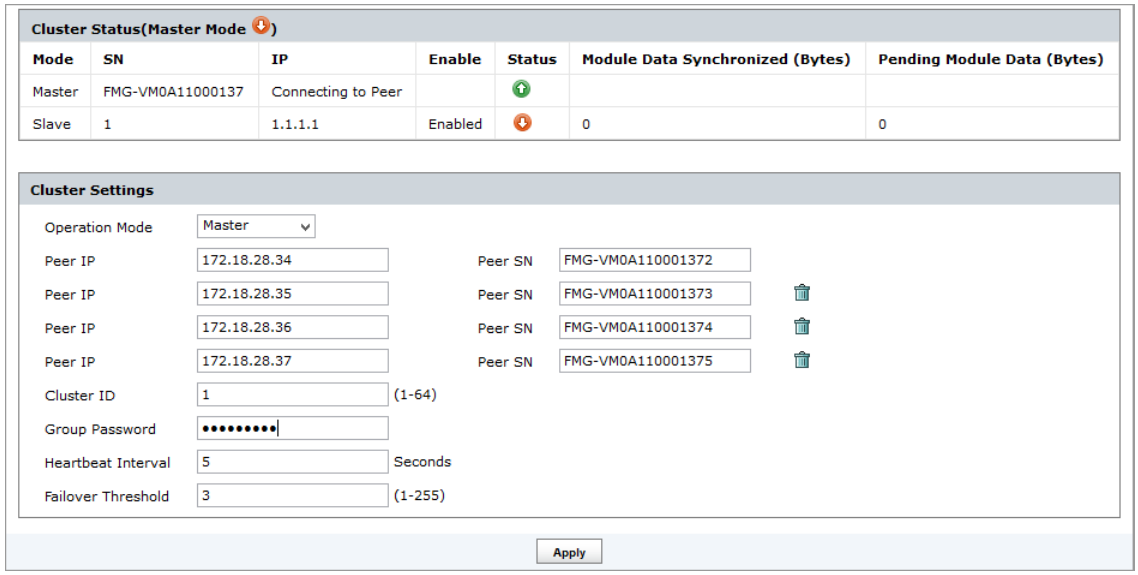
To configure HA options go to *System Settings* > *HA*. From here you can configure FortiManager units to start an HA cluster or you can change the HA configuration of the cluster.

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

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

You can connect to the primary unit 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 304: Cluster settings



Configure the following settings:

Cluster Status	Monitor FortiManager HA status. See "Monitoring HA status" on page 477.
Mode	The high availability mode, either *Master* or *Slave*.
SN	The serial number of the device.
IP	The IP address of the device.
Enable	Shows if the peer is currently enabled.
Status	The status of the cluster member.
Module Data Synchronized	Module data synchronized represented in Bytes.
Pending Module Data	Pending module data represented in Bytes.
Cluster Settings	
Operation Mode	Select *Master* to configure the FortiManager unit to be the primary unit in a cluster. Select *Slave* to configure the FortiManager unit to be a backup unit in a cluster. Select *Standalone* to stop operating in HA mode.
Peer IP	Enter the IP address of another FortiManager unit in the cluster. For the primary unit you can add up to four Peer IPs for up to four backup units. For a backup unit you add the IP address of the primary unit.
Peer SN	Enter the serial number of another FortiManager unit in the cluster. For the primary unit you can add up to four Peer serial numbers for up to four backup units. For a backup unit you add the serial number of the primary unit.

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

General FortiManager HA configuration steps

The following procedures assume that you are starting with four FortiManager units running the same firmware build and are set to the factory default configuration. The primary unit and the first backup unit are connected to the same network. The second backup units is connected to a remote network and communicates with the primary unit over the Internet.

1. Configure the FortiManager units for HA operation:
   - Configure the primary unit.
   - Configure the backup units.
2. Change the network configuration so that the remote backup unit and the primary unit can communicate with each other.
3. Connect the units to their networks.

4. Add basic configuration settings to the cluster:
   - Add a password for the admin administrative account.
   - Change the IP address and netmask of the port1 interface.
   - Add a default route.

Web-based Manager configuration steps

Use the following procedures to configure the FortiManager units for HA operation from the FortiManager unit Web-based Manager. Sample configuration settings are also shown.

To configure the primary unit for HA operation:

1. Connect to the primary unit Web-based Manager.
2. Go to *System Settings* > *HA*.
3. Configure HA settings.

   Example HA master configuration:

Operation Mode	Master
Peer IP	172.20.120.23
Peer SN	<serial_number>
Peer IP	192.268.34.23
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4. Select *Apply*.
5. Power off the primary unit.

To configure the backup unit on the same network for HA operation:

1. Connect to the backup unit Web-based Manager.
2. Go to *System Settings* > *HA*.
3. Configure HA settings.

   Example local backup configuration:

Operation Mode	Slave
Priority	5 (Keep the default setting.)
Peer IP	172.20.120.45
Peer SN	<serial_number>
Cluster ID	15
Group Password	password

Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4. Select *Apply*.
5. Power off the backup unit.

To configure a remote backup unit for HA operation:

1. Connect to the backup unit Web-based Manager.
2. Go to *System Settings* > *HA*.
3. Configure HA settings.

   Example remote backup configuration:

Operation Mode	Slave
Priority	5 (Keep the default setting.)
Peer IP	192.168.20.23
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4. Select *Apply*.
5. Power off the backup unit.

To change the network configuration so that the remote backup unit and the primary unit can communicate with each other:

Configure the appropriate firewalls or routers to allow HA heartbeat and synchronization traffic to pass between the primary unit and the remote backup unit using the peer IPs added to the primary unit and remote backup unit configurations.

HA traffic uses TCP port 5199.

To connect the cluster to the networks:

1. Connect the cluster units.

   No special network configuration is required for the cluster.
2. Power on the cluster units.

   The units start and user HA heartbeat packets to find each other, establish the cluster, and synchronize their configurations.

To add basic configuration settings to the cluster:

Configure the cluster to connect to your network as required.

Monitoring HA status

Go to *System Settings* > *HA* to monitor the status of the FortiManager units in an operating HA cluster. The FortiManager HA status dialog box displays information about the role of each cluster unit, the HA status of the cluster, and also displays the HA configuration of the cluster.



The FortiManager Web-based Manager browser window title changes to indicate that the FortiManager unit is operating in HA mode. The following text is added to the title *HA (Group ID: <group_id>)*. Where <group_id> is the HA Group ID.



From the FortiManager CLI you can use the command `get system ha` to display the same HA status information.

Figure 305: FortiManager HA status

Cluster Status(Master Mode)

Mode	SN	IP	Enable	Status	Module Data Synchronized (Bytes)	Pending Module Data (Bytes)
Master	FMG-VM0A11000137	Connecting to Peer				
Slave	1234567890	172.20.120.45	Enabled		0	0
Slave	1234567891	192.168.20.23	Enabled		0	0
Slave	032165487945	1.2.3.4	Enabled		0	0

The following information is displayed:

Mode	The role of the FortiManager unit in the cluster. The role can be: • *Master*: for the primary (or master) unit. • *Slave*: for the backup units.
Cluster Status	The cluster status can be *Up* if this unit is received HA heartbeat packets from all of its configured peers. The cluster status will be *Down* if the cluster unit is not receiving HA heartbeat packets from one or more of its configured peers.
Module Data Synchronized	The amount of data synchronized between this cluster unit and other cluster units.
Pending Module Data	The amount of data waiting to be synchronized between this cluster unit and other cluster units.

Upgrading the FortiManager firmware for an operating cluster

You can upgrade the FortiManager firmware of an operating FortiManager cluster in the same was a upgrading the firmware of a standalone FortiManager unit. During the firmware upgrade procedure, you connect to the primary unit Web-based Manager or CLI to upgrade the firmware. Then install the firmware on the slave units.

Similar to upgrading the firmware of a standalone FortiManager unit, normal FortiManager operations are temporarily interrupted while the cluster firmware upgrades. As a result of this interruption, you should upgrade the firmware during a quiet period.

To upgrade FortiManager HA cluster firmware:

1. Log into the primary unit Web-based Manager.
2. Upgrade the primary unit firmware.

   The firmware is forwarded to all the slave units, and then all the devices (master and slaves) are rebooted.

   See "FortiManager Firmware" on page 479 for more information.

Administrators may not be able to connect to the FortiManager Web-based Manager until the upgrade synchronization process is complete. During the upgrade, using SSH or telnet to connect to the CLI may also be slow, however use the console to connect to the CLI.

FortiManager Firmware

This section explains how to properly upgrade to FortiManager v5.0 Patch Release 5. The following topics are included in this section:

- Upgrading from FortiManager v5.0.0 or later
- Upgrading from FortiManager v4.0 MR3
- General firmware upgrade steps
- Upgrading the FortiManager firmware for an operating cluster
- Downgrading to previous firmware versions
- This section highlights some of the operational changes that administrators should be aware of in FortiManager v5.0 Patch Release 5.



Please review the *FortiManager v5.0 Patch Release 5 Release Notes* prior to upgrading your FortiManager device.



You can download the FortiManager MIB file in the firmware image FTP directory. The Fortinet Core MIB file is located in the main FortiManager v5.00 directory.



Firmware best practice: Stay current on patch releases for your current major release. Only upgrade to a new major release or version when you are looking for specific functionality in the new major release or version. For more information, see the *FortiManager Release Notes* or contact Fortinet Customer Service & Support.

Upgrading from FortiManager v5.0.0 or later

FortiManager v5.0 Patch Release 5 officially supports upgrade from FortiManager v5.0.0 or later.

Upgrading from FortiManager v4.0 MR3

FortiManager v5.0 Patch Release 5 officially supports upgrade from FortiManager v4.0 MR3.

General firmware upgrade steps

The following table lists the general firmware upgrade steps.

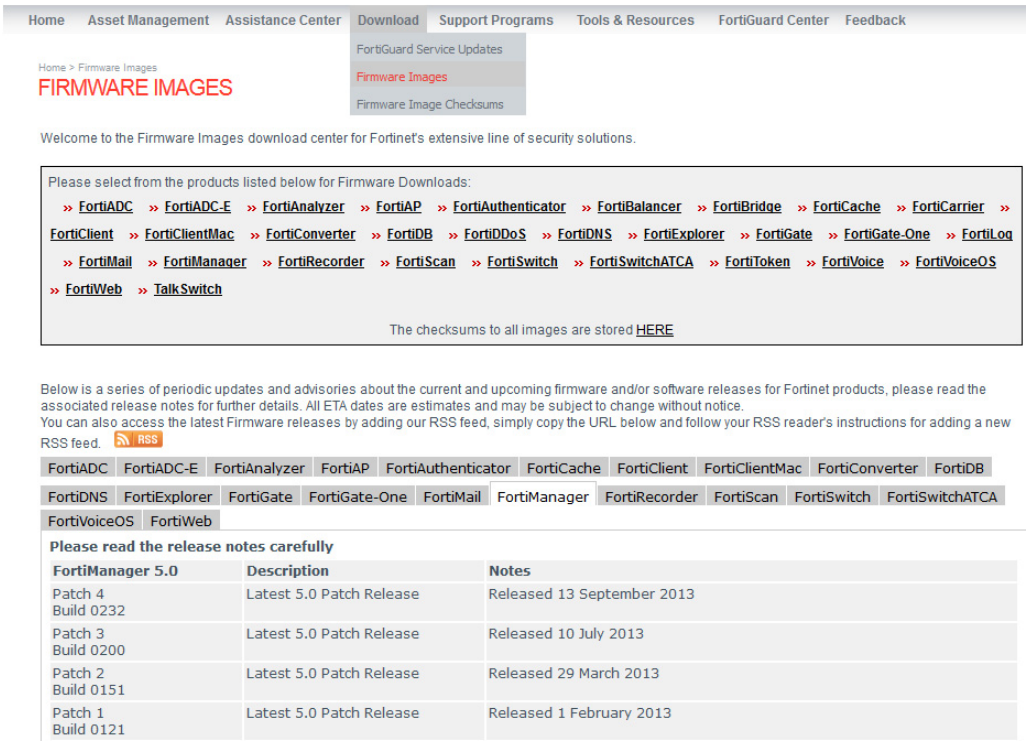
Table 16: Upgrade steps

Step 1	Prepare your FortiManager for upgrade.
Step 2	Backup your FortiManager system configuration. For FortiManager VM, take a *Snapshot* of the VM instance.
Step 3	Transfer the FortiManager firmware image to your FortiManager device.
Step 4	Log into your FortiManager Web-based Manager to verify the upgrade was successful.

Step 1: Prepare your FortiManager for upgrade

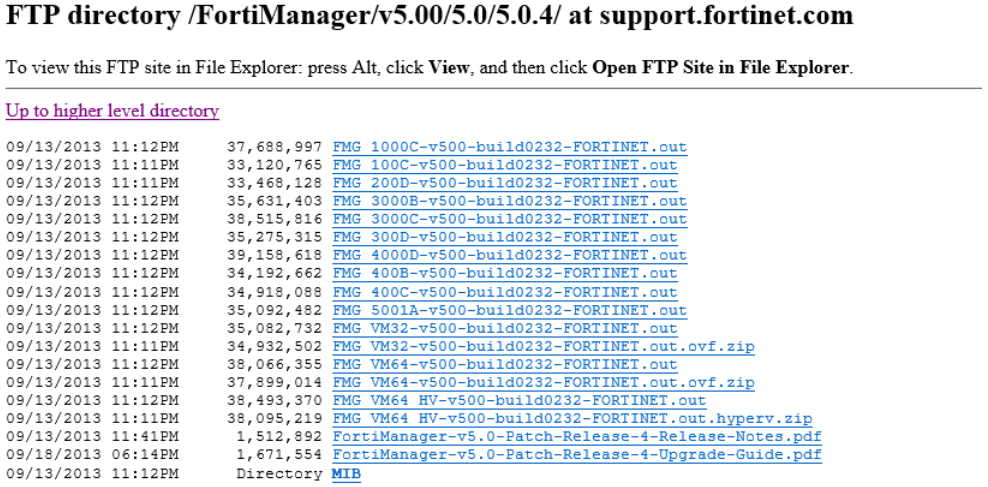
1. Install any pending configurations.
2. Make sure all managed devices are running the supported firmware versions as stated in the *FortiManager Release Notes*.
3. Log in to the Customer Service & Support portal at https://support.fortinet.com.
4. In the *Download* section of the page, select *Firmware Images*, and select *FortiManager.* Optionally, you can select *Download* in the toolbar and select *Firmware Images* from the drop-down list.

Figure 306: Firmware images page



5. Browse to the appropriate FTP directory to download the device specific firmware image and *FortiManager Release Notes* document.

Figure 307: Example FTP directory



FTP directory /FortiManager/v5.00/5.0/5.0.4/ at support.fortinet.com

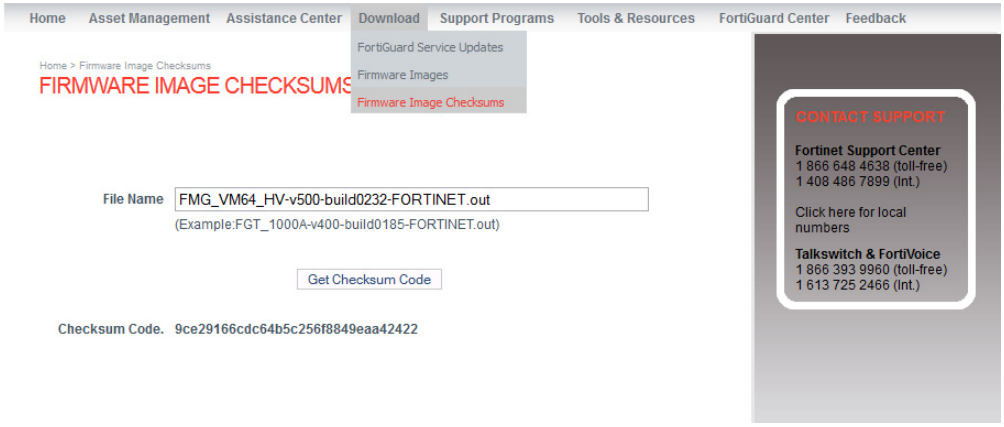
To view this FTP site in File Explorer: press Alt, click **View**, and then click **Open FTP Site in File Explorer**.

Up to higher level directory

```
09/13/2013 11:12PM     37,688,997 FMG_1000C-v500-build0232-FORTINET.out
09/13/2013 11:11PM     33,120,765 FMG_100C-v500-build0232-FORTINET.out
09/13/2013 11:11PM     33,468,128 FMG_200D-v500-build0232-FORTINET.out
09/13/2013 11:12PM     35,631,403 FMG_3000B-v500-build0232-FORTINET.out
09/13/2013 11:12PM     38,515,816 FMG_3000C-v500-build0232-FORTINET.out
09/13/2013 11:12PM     35,275,315 FMG_300D-v500-build0232-FORTINET.out
09/13/2013 11:12PM     39,158,618 FMG_4000D-v500-build0232-FORTINET.out
09/13/2013 11:12PM     34,192,662 FMG_400B-v500-build0232-FORTINET.out
09/13/2013 11:12PM     34,918,088 FMG_400C-v500-build0232-FORTINET.out
09/13/2013 11:12PM     35,092,482 FMG_5001A-v500-build0232-FORTINET.out
09/13/2013 11:12PM     35,082,732 FMG_VM32-v500-build0232-FORTINET.out
09/13/2013 11:11PM     34,932,502 FMG_VM32-v500-build0232-FORTINET.out.ovf.zip
09/13/2013 11:12PM     38,066,355 FMG_VM64-v500-build0232-FORTINET.out
09/13/2013 11:11PM     37,899,014 FMG_VM64-v500-build0232-FORTINET.out.ovf.zip
09/13/2013 11:12PM     38,493,370 FMG_VM64_HV-v500-build0232-FORTINET.out
09/13/2013 11:11PM     38,095,219 FMG_VM64_HV-v500-build0232-FORTINET.out.hyperv.zip
09/13/2013 11:41PM      1,512,892 FortiManager-v5.0-Patch-Release-4-Release-Notes.pdf
09/18/2013 06:14PM      1,671,554 FortiManager-v5.0-Patch-Release-4-Upgrade-Guide.pdf
09/13/2013 11:12PM      Directory MIB
```

6. To verify the integrity of the download, go back to the *Download* section of the login page, then select the *Firmware Image Checksums* link. Optionally, you can select *Download* in the toolbar and select *Firmware Image Checksums* from the drop-down list.

Figure 308: Firmware image checksum page



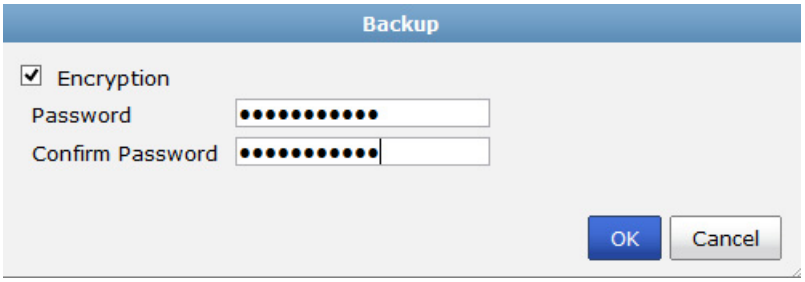
7. Enter the file name and select *Get Checksum Code* to get the firmware image checksum code. Compare this checksum with the checksum of the firmware image.

Step 2: Backup your FortiManager system configuration

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

The *Backup* dialog box opens.

Figure 309: Backup dialog box



3. Select the checkbox to encrypt the backup file and enter a password.

When selecting to encrypt the backup configuration file, the same password used to encrypt the file will be required to restore this backup file to the FortiManager device.

4. Select *OK* and save the backup file on your management computer.

The system configuration file from a FortiManager v4.0 MR3 device cannot be directly imported into a FortiManager v5.0 Patch Release 5 device.

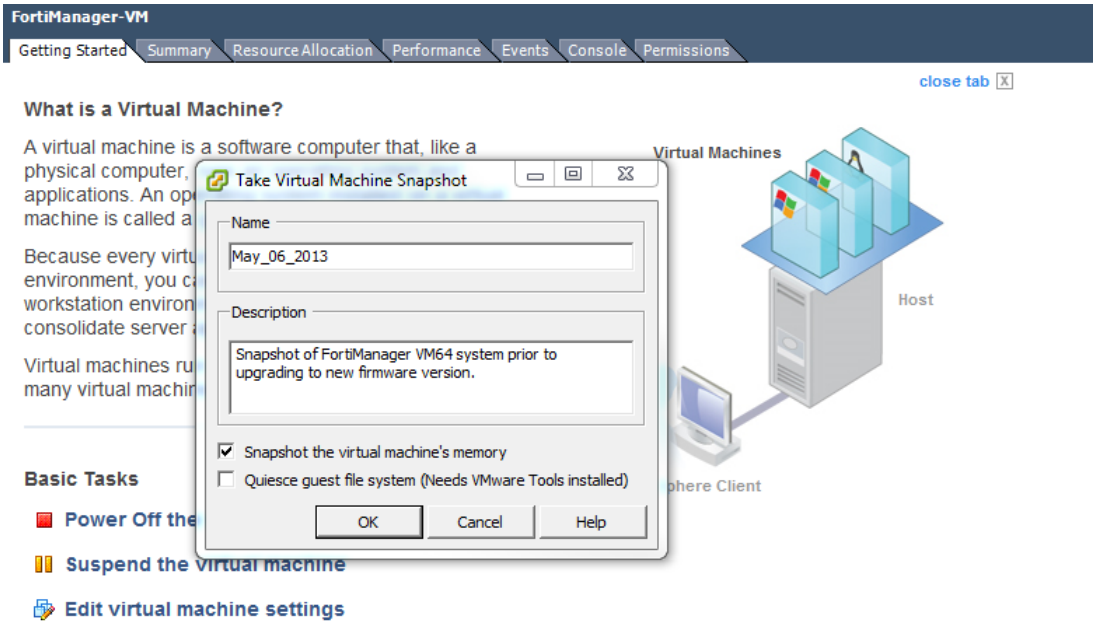
Optionally, you can backup the configuration file to a FTP, SFTP, or SCP server using the following CLI command:

```
execute backup all-settings {ftp | sftp} <ip> <path/filename save to
    the server> <username on server> < password> <crptpasswd>
execute backup all-settings scp <server IP address> <path/filename
    save to the server> <SSH certificate> <crptpasswd>
```

For more information, see the *FortiManager v5.0 Patch Release 5 CLI Reference*.

5. In VM environments, it is recommended that you take a *Snapshot* of the VM instance. In the event of an issue with the firmware upgrade, use the *Snapshot Manager* to revert to the *Snapshot*. To create a *Snapshot*, right-click the VM instance and select *Snapshot* > *Take Snapshot*.

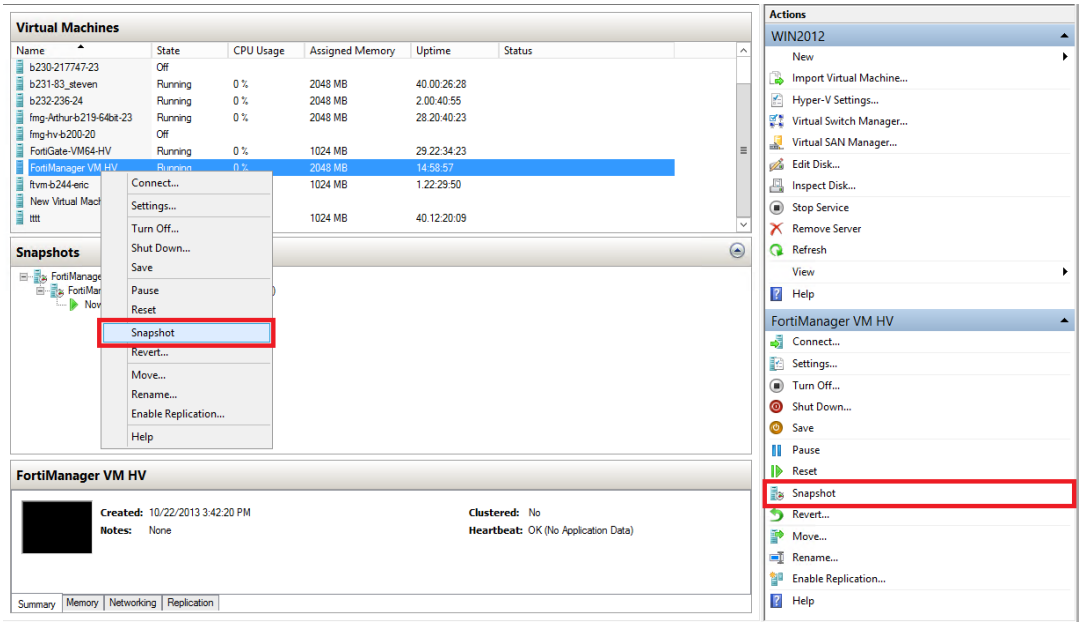
Figure 310: Snapshot of FortiManager VM (VMware)





For information on snapshots in Microsoft Hyper-V Server environments, refer to the Microsoft Windows Server online help.0256

Figure 311: Snapshot of FortiManager VM (Microsoft Hyper-V)

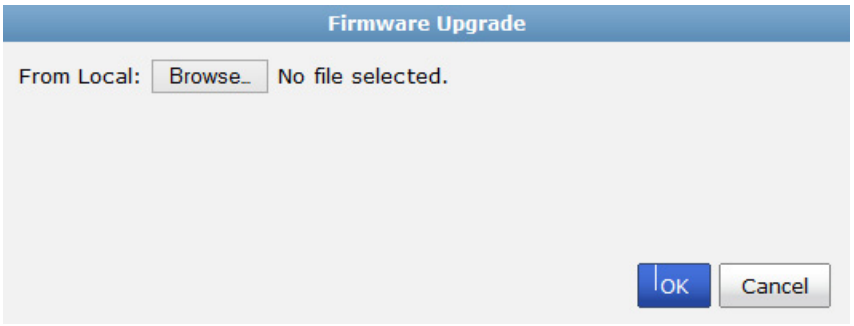


Step 3: Transfer the firmware image to your FortiManager device

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Firmware Version* field, select *Update*.

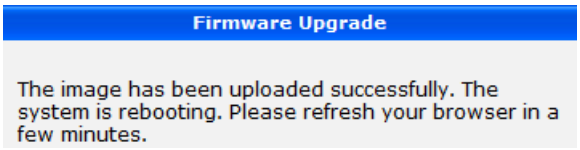
   The *Firmware Update* dialog box opens.

Figure 312: Firmware upgrade dialog box



3. Select *Browse* to locate the firmware image (`.out` file) that you downloaded from the Customer Service & Support portal and select *Open*.
4. Select *OK*. Your FortiManager will upload the firmware image and you will receive the following message.

Figure 313: Firmware upgrade successful dialog box





Optionally, you can upgrade firmware stored on an FTP or TFTP server using the following CLI command:

```
execute restore image {ftp | tftp} <file path to the server> <server
    ip address> <username on server> <password>
```

For more information, see the *FortiManager v5.0 Patch Release 5 CLI Reference*.

Step 4: Verify the upgrade

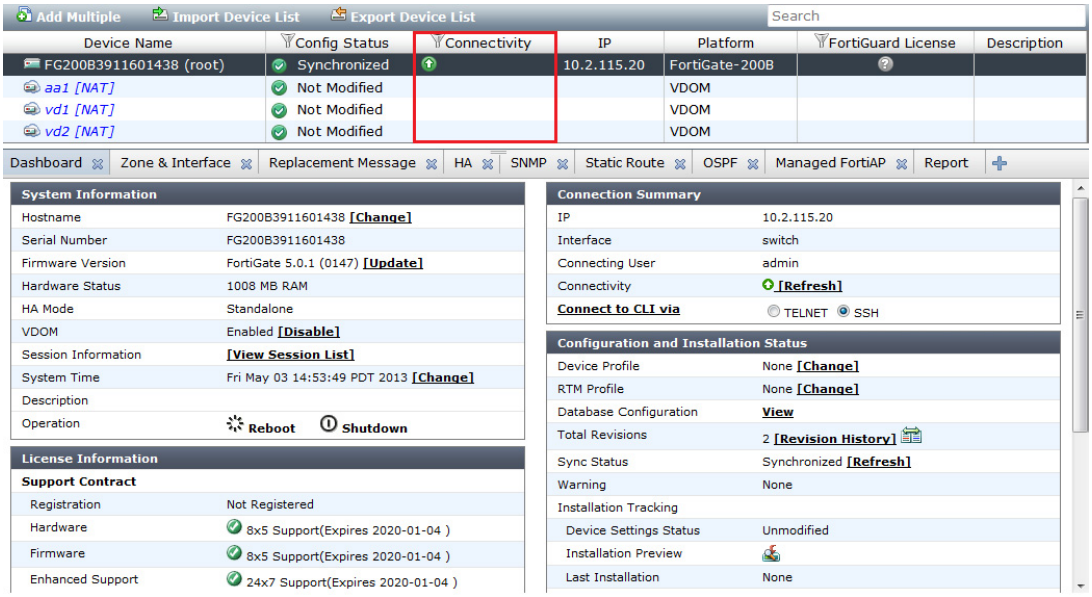
1. Refresh the browser and log back into the device.



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.

2. Launch the *Device Manager* module and make sure that all formerly added devices are still listed.
3. Select each ADOM and make sure that managed devices reflect the appropriate connectivity state. Optionally, go to *System Settings* > *General* > *All ADOMs*.

Figure 314: Verify device connectivity



4. Launch other functional modules and make sure they work properly.

Upgrading the FortiManager firmware for an operating cluster

You can upgrade the FortiManager firmware of an operating FortiManager cluster in the same was a upgrading the firmware of a standalone FortiManager unit. During the firmware upgrade procedure, you connect to the primary unit Web-based Manager or CLI to upgrade the firmware.

Similar to upgrading the firmware of a standalone FortiManager unit, normal FortiManager operations are temporarily interrupted while the cluster firmware upgrades. As a result of this interruption, you should upgrade the firmware during a maintenance window.

To upgrade FortiManager HA cluster:

1. Log into the primary unit's Web-based Manager using the `admin` administrator account.
2. Upgrade the primary unit's firmware. The upgrade is synchronized between the primary device and backup devices.

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.

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous FortiManager firmware release via the Web-based Manager or CLI. A system reset is required after the firmware downgrading process has completed.



All configuration will be lost after downgrading the device. For FortiManager devices with hard drives installed, the hard drives will be formatted.

To re-initialize a FortiManager use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```

Special notices

This section highlights some of the operational changes that administrators should be aware of in FortiManager v5.0 Patch Release 5.

FortiOS features currently not supported by FortiManager

The following features in FortiOS v5.0 Patch Release 5 are not supported in FortiManager v5.0 Patch Release 5:

- Updated categories within the application sensor
- Mobile FortiToken support
- FortiManager should support SSL VPN custom login
- Add *More Filters* options for IPS and Application Control profiles
- Add Web Filter administrative override Web-based Manager support

FortiGate firmware upgrade

After completing a FortiGate firmware upgrade via FortiManager, you must manually retrieve the device configuration.

System time on FortiManager VM

If an NTP server is not reachable from a FortiManager VM unit, it will use the VMware ESX/ESXi host's time as the system time.

Memory requirement for FortiManager VM64-HV

A minimum of 2GB of memory is required to normally operate FortiManager VM64-HV (Microsoft Hyper-V).

ADOM for FortiCarrier

Please note that FortiGate and FortiCarrier devices can no longer be grouped into the same ADOM in FortiManager v5.0 Patch Release 5. FortiCarrier devices should be grouped into a dedicated FortiCarrier ADOM.

After upgrade, FortiCarrier devices will no longer be shown in any of the existing ADOMs. When creating a FortiCarrier ADOM, the FortiCarrier devices will be listed and can be grouped into the ADOM.



ADOM mode must be enabled in order to create a FortiCarrier ADOM and manage FortiCarrier devices.

FortiOS v5.0 override server setting for FortiGuard Services

FortiOS no longer has the option to specify an IP address or a domain name for FortiGuard services. FortiGate either connects to the FortiGuard Distribution Network or the managing FortiManager for update services. If a FortiGate is required to retrieve updates from a specific FortiManager or FortiGuard server, please use port address translation (PAT) to redirect update traffic to the proper IP address and port. Table 17 lists the ports used by FortiGuard Services.

Table 17: FortiGuard services ports

Port	Service
8890	Antivirus or IPS updates for FortiGate
53 or 8888	Web Filtering or Antispam queries for FortiGate
8891	Antivirus or IPS updates for FortiClient
80	Web Filtering or Antispam queries for FortiClient

The public FortiGuard uses port 443 to provide antivirus/IPS updates. On FortiManager, it uses port 8890 (FortiGate) / port 8891 (FortiClient) instead. See the two examples below.

Example 1: Antivirus/IPS

In this example, the FortiGate (10.1.100.1) is managed by FortiManager1 (172.16.200.102) and gets antivirus/IPS updates from FortiManager2 (172.16.200.207). A NAT/PAT device (10.1.100.2/172.16.200.2) sits between the FortiGate and the FortiManager.

On the FortiGate, enter the following CLI commands to enable FortiManager FDS override and set the FortiManager IP address (internal IP on NAT/PAT device):

```
config system central-management
  set fortimanager-fds-override enable
  set fmg "10.1.100.2"
end
```

On the NAT/PAT device, configure the following IP and port translations:

```
10.1.100.2:8890 -> 172.16.200.207:8890
10.1.100.2:541 -> 172.16.200.102:541
```

Example 2: Web filtering/Antispam

In this example, the FortiGate (10.1.100.1) is managed by FortiManager1 (172.16.200.102) and performs web filtering and antispam queries on FortiManager2 (172.16.200.207). A NAT/PAT device (10.1.100.2/172.16.200.2) sits between the FortiGate and the FortiManager.

On the FortiGate, enter the following CLI commands to enable FortiManager FDS override and set the FortiManager IP address (internal IP on NAT/PAT device):

```
config system central-management
  set fortimanager-fds-override enable
  set fmg "10.1.100.2"
end
```

On the NAT/PAT device, configure the following IP and port translations:

```
10.1.100.2:53/8888 -> 172.16.200.207:53/8888
10.1.100.2:541 -> 172.16.200.102:541
```

Update services provided to FortiGate v4.0 MR2 or FortiMail devices

Please enable the following option in order to provide update services to FortiGate v4.0 MR2 and FortiMail devices:

```
config fmupdate support-pre-fgt43
  set status enable
end
```

Log arrays

After creating a log array, only new logs will be populated into this array. Older logs will remain on the device. To collect older logs, you will need to build the array database. Use the following CLI command to build the array database:

```
execute sql-local rebuild-device <log array device ID>
```

The SQL logs for the members of the log array will be rebuilt. To verify that the array rebuild was successful, select the *Log View* tab to view the log array and logs.



Executing this command will not reboot the FortiManager device.



Fortinet recommends configuring log arrays prior to deploying the FortiManager into production. When adding and deleting log arrays, you will need to rebuild the database to view older logs.

Endpoint management

In version 5.0, FortiClient endpoint agent configuration and management are now handled by the FortiGate Endpoint Control feature. You can configure your FortiGate device to discover new devices on your network, enforce FortiClient registration, and deploy a pre-configured endpoint profile to connected devices. This feature requires a FortiGate device running FortiOS v5.0.0 or later.

For more information, see the *Device and Client Reputation for FortiOS 5.0 Handbook* available at http://docs.fortinet.com.

FortiManager VM license check

As a part of the license validation process FortiManager compares its IP addresses with the IP information in the license file. If the IP addresses do not match, FortiManager returns the error `IP does not match` within CLI command `get system status` output. If a new license has been imported or the FortiManager's IP address has been changed, the FortiManager must be manually rebooted in order for the system to validate the change and operate with a valid license.

Multi-language display support

FortiManager v5.0 Patch Release 1 or later has restrictions on supporting a FortiGate device's multi-language display.

New hard disk drive partition layout

FortiManager v5.0.0 introduced a new hard disk drive partition layout which is required for optimal usage and performance. Following an upgrade to FortiManager v5.0.0 or later, a backup must be made and then the disk must be reformatted with following command:

```
execute format {disk | disk-ext4}
```

A format will erase all local logs, and FortiGuard database information. Backup any local event logs that you wish to keep. The FortiManager will then need to re-download all of the AV/IPS/AS/WF objects from the FortiGuard Distribution Servers (FDS) which may take up to half a day. During that time managed devices will not be able to obtain these services from the FortiManager. You should configure devices to point to a backup FortiManager or the FDS for these services.

Importing a FortiManager generated policy

FortiManager has the option to import all policies from a FortiGate device into a single policy package. Due to design limitations, the import process removes all policies with FortiManager generated policy IDs, such as 1073741825, that previously were learned by a FortiManager unit. The FortiGate unit may inherit a policy ID from:

- Global Header Policy
- Global Footer Policy
- VPN Console

Importing profile group and RADIUS dynamic start server

Please be advised that the *Import Wizard* does not import profile group and RADIUS dynamic start server objects which are not referenced by firewall policies. Please configure those objects on your FortiManager device.

Push update in bi-directional static NAT

Whenever there is a NAT device between FortiGate devices and the FortiManager with bi-directional static NAT enabled, you must follow the instructions below in order for FortiGate devices to receive *Push Update* announcements from the FortiManager.

Configure the following settings on FortiManager:

```
config fmupdate av-ips push-override-to-client
  set status enable
  config announce-ip
    edit 1
      set ip <the override IP that the FortiGate uses to download
           updates from the FortiManager>
      set port <the port that the FortiManager uses to send the
           update announcement>
    end
  end
end
```

Appendix A: FortiManager VM

Licensing

Fortinet offers the FortiManager VM in a stackable license model. This model allows you to expand your VM solution as your environment expands. When configuring your FortiManager VM, ensure to configure hardware settings as outlined in Table 18 and consider future expansion. Contact your Fortinet Authorized Reseller for more information.

Table 18: FortiManager license information

Technical Specification	VM-BASE	VM-10-UG	VM-100-UG	VM-1000-UG	VM-5000-UG	VM-U-UG
Hypervisor Support	VMware ESX versions 4.0 and 4.1 VMware ESXi versions 4.0, 4.1, 5.0, and 5.1 Microsoft Hyper-V Server 2008 R2 and 2012					
VM Form Factor	VMware ESX/ESXi: Open Virtualization Format (OVF) Microsoft Hyper-V Server: Virtual Hard Disk (VHD)					
HA Support	Yes					
Virtual CPUs (Min / Max)	1 / Unlimited					
Virtual Network Interfaces (Min / Max)	1 / 4					
Virtual Memory (Min / Max)	2GB / 4GB for 32-bit and 2GB/ Unlimited for 64-bit					
Virtual Storage (Min / Max)	80GB / 16TB					
GB / Day of logs	1	2	5	10	25	50
Device Quota	100GB	200GB	1TB	4TB	8TB	16TB

For more information see the FortiManager product datasheet available on the Fortinet web site, http://www.fortinet.com/products/fortimanager/virtualappliances.html.

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for both VMware ESX/ESXi and Microsoft Hyper-V Server virtualization environments.

VMware ESX/ESXi

- `.out`: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.ovf.zip`: Download either the 32-bit or 64-bit package for a new FortiManager VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.



Fortinet recommends upgrading your VMware ESXi 4.1 server to VMware ESXi 4.1 Update 3, version 4.1.0 U3, build 800380 or later before installing or upgrading FortiManager VM to avoid server instability or purple diagnostic screen issues.

Microsoft Hyper-V Server

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

Appendix B: Maximum Values

FortiManager maximum values

The following table provides a detailed summary of maximum values on FortiManager platforms.

Table 19: FortiManager maximum values

FortiManager Platform	Devices[2]	Max ADOMs	Max Web Portal / Users
FMG-200D	30	30	-
FMG-300D	300	300	
FMG-400C	300	300	-
FMG-1000C	800	800	800
FMG-1000D	1,000	1,000	1,000
FMG-3000C	5,000	5,000	5,000
FMG-4000D	4,000	4,000	4,000
FMG-5001A	4,000	4,000	4,000
FMG-VM-Base	10	10	10
FMG-VM-10	+10	+10	+10
FMG-VM-100	+100	+100	+100
FMG-VM-1000	+1,000	+1,000	+1,000
FMG-VM-5000	+5,000	+5,000	+5,000
FMG-VM-U	Unlimited[1]	Unlimited[1]	Unlimited[1]

[1] Limited in software to 10,000 devices, ADOMs, Web Portals, and Web Portal users.
[2] Each VDOM operating on a physical device counts as one (1) licensed network device.

Appendix C: License Information API

The FortiManager API enables you to configure managed FortiGate devices through a web services interface. See the *FortiManager XML API Reference* on the Fortinet Developer Network portal for more information.

The XML API `getDeviceLicenseList` has been added for generating and downloading license information for services on each managed device.

The data is gathered from the update manager, as opposed to individual devices in the device manager. The update manager reports what subscriptions are currently available.

The generated file contains the device serial number, and the expiry date of each service, including the support contract and various services, such as AV, IPS, and web filter.

getDeviceLicenseList

Use this request to obtain a list of device licenses.

Request Field	Description
`<servicePass>`	XML structure consists of username and password variables.
`<userID>`	The administrator user name.
`<password>`	Administrator password options: • Enter the administrator password. • Leave field blank for no password.

Example request:

```
<soapenv:Envelope xmlns:soapenv="http://..." xmlns:r20="http://.../">
  <soapenv:Header/>
  <soapenv:Body>
    <r20:getDeviceLicenseList>
      <!--Optional:-->
      <servicePass>
        <!--Optional:-->
        <userID>admin</userID>
        <!--Optional:-->
        <password></password>
      </servicePass>
    </r20:getDeviceLicenseList>
  </soapenv:Body>
</soapenv:Envelope>
```

The response includes the device serial number, support type, support level, and expiry date.

Response Field	Description
<serial_number>	The device serial number.
<support_type>	Support contract types include: • AVDB: Antivirus Signature Definition Update Support • AVEN: Antivirus Engine Update Support • COMP: Comprehensive Support • ENHN: Enhancement Support • FMWR: Firmware Update Support • FRVS: FortiScanner Database Update Support • FURL: Web Filtering Support • SPAM: AntiSpam Support • HDWR: Hardware Support • NIDS: Intrusion Detection Support • SPRT: Technical Support via Telephone • VCME: FortiGate Network scanner plugin
<support_level>	Support levels include: • 99: Trial contract • 10: 8x5 support contract • 20: 24x7 support contract
<expiry_date>	Support contract expiry date.

Example response

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
  <ns3:getDeviceLicenseListResponse>
    <return>
      <device>
        <serial_number>FE100C3909000002</serial_number>
        <contract>
          <support_type>AVDB</support_type>
          <support_level>10</support_level>
          <expiry_date>20120824</expiry_date>
        </contract>
        <contract>
          <support_type>AVEN</support_type>
          <support_level>10</support_level>
          <expiry_date>20120824</expiry_date>
        </contract>
        <contract>
          <support_type>NIDS</support_type>
          <support_level>10</support_level>
          <expiry_date>20120824</expiry_date>
```

```
            </contract>
            <contract>
              <support_type>SPAM</support_type>
              <support_level>10</support_level>
              <expiry_date>20120824</expiry_date>
            </contract>
            <contract>
              <support_type>SPRT</support_type>
              <support_level>20</support_level>
              <expiry_date>20120824</expiry_date>
            </contract>
            <contract>
              <support_type>FRVS</support_type>
              <support_level>10</support_level>
              <expiry_date>20120824</expiry_date>
            </contract>
          </device>
        </return>
      </ns3:getDeviceLicenseListResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Index

A

access
  public servers 459
  rules 278
acknowledge
  events 385
add
  break 417
  chart 411
  chassis 172
  device 148, 209
  elements 408–417
  event handler 389, 391
  external users 276
  hard disk 84
  headings 414
  IPv6 static route 89
  language 441
  logo 275
  model device 208
  report cover 411
  script 245
  template image 413
  text box 415
  VDOM 219
  web portal content 273
  web portal profile 272
  web portal user 276
  widget 60
address 350
  override 450, 451
administration
  changing access 45
  session timeout 93
administrative domain. See ADOM
administrator 94
  access 41
  access profiles 92
  accounts 92
  add account 95
  authentication server 92
  configure 94
  connection options 92
  current 63
  delete 93, 97
  disconnect 93
  modify 97
  monitoring 92
  netmask 96
  new 33
  profiles 98
  settings 105
  trusted host 97
administrator profiles
  delete 100
  modify 100
ADOM 37, 48, 279
  access 131
  add device 148
  administrators 56
  advanced mode 55
  assign administrator 56
  assigning devices 55
  backup 50
  concurrent access 31, 52
  create new 52, 53
  delete 54
  device modes 55
  disable 49
  enable 49, 63
  file format 153
  FortiMail 49
  FortiWeb 49
  global layer 39
  layer 39
  lock 31, 56, 131, 284, 291
  lock override 31, 52
  mode 54
  name 53
  navigation 129
  normal mode 50
  organize 48
  revisions 333, 334, 335
  switching between 50
  upgrade 51, 54
  version 24, 51, 80
advanced
  settings 114, 127
  system settings 114
alerts
  email events 393
  mail server 121
  message console 74
  syslog server 122
antispam 460
antivirus 278, 350, 443, 455
  enable 445, 448
  query 460
  settings 449
  update 450
API 127, 494
archive
  logs 370

assign
administrator 56
client reputation profile 203
devices 55
global policy package 286
authentication
proxy 456
remote 101
server 92

B

backup 66
configuration 63
encrypt 67
backup mode 54
bind
zone 32
browse
log 371
built-in
FDS 454, 456

C

calendar 434
certificate 107
add device 204
create 108
create new 203
delete 204
download 111
edit 204
generate 205
import 109
template 203
view details 109, 110
certificate revocation list. See CRL
change
date 64
encryption mode 73
host name 63
serial number 149
time 64
chart
advanced options 430
builder 426
category 431
clone 432
configure 430
create new 431
dataset 431
delete 433
edit 433
filters 427
name 431
template 426
type 429
wizard 426
chassis
add 172
dashboard 173
edit 173
enable management 127, 171
fan tray 173
manage 171
managing 171
PEM 173, 174
SAP 173
shelf manager 173
check
consistency 289
checkmark 454
checkpoint 68
create 68, 69
CLI 59, 60, 148, 242
commands 76
console 75, 177
more 255
client reputation 202
client reputation profile
assign 203
edit 202
new 202
threat level 202
clone
chart 432
dataset 436
endpoint profile 201
event handler 394
object 356
policy 330
report template 407
script 246
SSID 184
WIDS profile 194
wireless profile 189
cluster
connect 476
network 476
settings 472
column
log view 368
order 368
columns
filter 132
settings 130
command line interface. See CLI
command prompt 63
community 116
name 117
configuration
comparing 240
history 37
managing revisions 238
restore 67
reverting 241

configuration file
downloading 240
importing 240
configure
admin settings 105
administrator 94
administrator profiles 99
backup 63, 66
backup unit 475
chart 430
date 64
device 159
device logs 126
encryption mode 73
event logging 125, 376
events 27, 383
FortiGuard services 455
FortiManager 41
FortiToken 357
HA 472, 474, 476
mail server 121
network interfaces 87
primary unit 475
profiles 32, 99
RAID 81
remote backup unit 476
resource limit 164
scripts 243
SNMP 115
SNMP community 116
syslog server 122
time 64
VDOMs 160
web portal 271
web portal profile 273
web proxy 453
connect
cluster 476
connection
handling 455
options 92
consistency check 289
perform 290
results 290
console 255
console access 97
copy
policy 331
corporate network 278
CPU utilization 71
create new
ADOM 52, 53
ADOM revision 334
certificate 108, 203
chart 431
client reputation profile 202
dataset 435
device group 170
device profile 179
endpoint profile 196
external users 276
identity policy 291, 301
log array 165
mail server 121
metadata 124
object 354
output profile 439
policy 291
policy folder 284
policy package 284
profiles 99
report template 406
schedule 33
script 245
section 331
SNMP community 116
SSID 179, 180
syslog server 122
template folder 408
VDOM 160
VDOM link 162
web portal profile 272
web portal user 276
WIDS profile 191, 192
wireless profile 186, 187
CRL 57, 107, 109
details 110
import 109
current
administrator 63
custom
chart 426
log view 367
profile 99
customize
dashboard 60
display 282
cut
policy 331

D

daily
log rolling 379
dashboard 132
chassis 173
customize 60
reset 61
system information 62
widget options 61

dataset
chart 431
clone 436
create new 435
delete 438
edit 437
report 434
SQL query 436, 438
date
configure 64
default
gateway 86
IP addresses 457
delete
administrator 93, 97
ADOM 54
ADOM revision 335
automatically 335
certificate 204
charts 433
datasets 438
device group 171
device profile 179
element 421
endpoint profile 201
event handler 394
firmware image 469
folder 286
languages 442
log array 166
log files 126
mail server 122, 123
metadata 124, 125
object 356
output profiles 441
policies 331
policy 286
profile 100
reports 425
schedule 422
script 247
SSID 179, 184
task 113
WIDS profile 191, 194
wireless profile 186, 189
destination
address 280
IP address 280
details
CA certificate 110
CRL 110
GB per day 73
local certificate 109
logs 369
device
add 147, 148, 209
configuration 31
configuring 159
dashboard 30
fail 471
file format 154
history 230
import 207
import policies 152
information 150
licenses 494
list 152
manager 38, 129, 455
model 208
modes 55
profile 31, 131, 177
refreshing 152
replace 148
settings 228
status 464
synchronization 30, 127
text file 153
unregistered 158
view 133
viewing 132
wizard 206
device group
add 170
delete 171
edit 171
device log
settings 114, 126
devices
assigning 55
unregistered 455
DHCP 456
diagnostic tools 90
differentiated services code point (DSCP)
originating traffic 295
reply traffic 295
disable
ADOMs 49
log rolling 378
log uploads 377, 378
schedule 423
workspaces 131
disconnected 453
discovery 209
disk 125
display
columns 368
customize 282
DNS 86
servers 86
dot3
Errors 119
Tests 119
downgrade
firmware 486

download
certificate 111
log 374
reports 425
WSDL file 127
drag and drop 350, 357
drill down 27
email activity 381
populated data 380, 381, 382
threat activity 382
traffic activity 380
web activity 381
dynamic
objects 350
search 357
dynamic object
map 354
view mappings 355

E

edit
administrator 97
ADOM revision 335
certificate 204
chart 433
chassis 173
client reputation profile 202
dataset 437
device 150
device group 171
device profile 179
element 420
endpoint profile 201
event handler 393
FortiAP 167
language 442
log array 166
mail server 122, 123
metadata 125
object 356
output profile 441
policy 330
policy package 286
report 420
schedule 422
script 246
SSID 184
temperature 174
template workspace 419
voltage 174
WIDS profile 194
wireless profile 189
element
add 408–417
delete 421
edit 420
move 420
email activity
drill down 381
email filter 443, 446, 449
enable 446, 448
update 450
enable
ADOMs 49, 63
chassis management 127, 171
email filter 446
event handler 395
log uploads 377
offline mode 127
push updates 455, 456
SNMP agent 116
VDOMs 160
web filter 446
workspaces 131
encrypt
backup 67
encryption
change mode 73
endpoint
templates 195
endpoint profile
clone 201
delete 201
edit 201
import 201
new 196
event
configure logging 376
logs 384
event details
acknowledge 384
raw logs 384
review notes 384
event handler 395
clone 386, 394
create 389, 391
create new 386
delete 386, 394
disable 386, 395
edit 386, 393
enable 386, 395
select all 386
traffic log 389
event logging
configure 125
event management 27
alert email 393
events 27, 383
FortiGate 383
FortiMail 383
FortiWeb 383
SNMP trap 393
syslog server 393
system event 393

events
acknowledge 385
configure 27, 383
event management 27, 383
monitor 383
severity 384
SNMP community 393
execute
script 244
export
device list 152, 153
policy 288
report template 407, 421
reports 27
script 247
external users 276
add 276

F

fail 458
device 471
fan tray 173
FDN 443, 444, 446, 455, 456, 457
connecting 453
disconnected 457
FDS 443, 444, 455, 456, 457, 460
built-in 454
connecting 453
logging 450
server 446, 451
FGFM 50
fields
meta 123
filter
columns 132
email 443, 446, 449
logs 369
scripts 242
web 443, 446, 449
filters
log type 392
FIN packet 304, 309, 316, 322, 328
firewall 271
firmware 278
downgrade 486
HA cluster 478
management 37
update 65, 168, 480
version 62
firmware images
delete 469
import 468
footer
policies 39
formatting 461
FortiAnalyzer 376
server 376
upload logs 198
VM 27
FortiAP
client list 168
edit 167
rogue AP list 169
update 168
FortiGate
configure 159
event management 383
managed 458
FortiGuard
antispam 447
antivirus settings 449
built-in FDS 454
center 455
connection status 457
default port 454
IPS settings 449
log settings 447
logging 450
override mode 446
private servers 447, 452
push updates 450, 456
server override 452
service licenses 443
services 455
update 450, 458
updates 450
web proxy 450, 452
FortiGuard Distribution Network. See FDN
FortiGuard Distribution Servers. See FDS
FortiMail 445, 446
ADOMs 49
event management 383
logging 26
reporting 26
support 26
FortiManager 20
configuring 41
reboot 47
shutdown 47
updates 199
upload logs 198
Fortinet
MIB 120
Fortinet Technical Support 65
FortiToken
configuration 357
FortiWeb
ADOMs 49
event management 383
logging 26
reporting 26
support 26
forward
port 456
FQDN 123
FTP
server 126
FTP server 376

G

generate
  certificate 205
geography 279
global
  database version 63
  objects 281
  policy package 284, 286
  policy packages 281
  VDOM resources 164
granularity 32
gray 454
green 453, 454
group
  add 170
  delete 171
  edit 171
  file format 155
gzip
  log file 126

H

HA 34, 90, 470, 491
  backup unit 475
  clusters 120, 472
  configuration 472, 474, 476
  heartbeat 471
  monitor 477
  primary unit 475
  remote backup 476
  start up 472
  status 62, 473
  synchronize 471
  upgrade firmware 478
handling
  connection attempts 455
hard disk 84
  add 84
  formatting 461
  usage 71
header
  policies 39
heartbeat
  interval 474
hide
  columns 368
high availability. See HA
historical reports 33
history 37, 230, 464, 466
  reports 424
  script 248, 249
  update 446
host name 62, 63
  change 63
hosts
  trusted 46
hot swap 84
HTTP 34, 45
  web proxy 456
HTTPS 34, 45, 454

I

identity policy
  create new 291
idle timeout 46, 106
import
  CA certificate 109
  CRL 109
  device 207
  device list 152, 153
  endpoint profile 201
  firmware image 468
  local certificate 109
  log 373
  policies 152
  report template 407, 421
  reports 27
  script 248
  SSID 179, 185
  text file 153
  WIDS profile 191, 194
  wireless profile 186, 189
  wizard 231
infrastructure 38
insert
  policy 330
install 31
  device settings 31, 224, 228
  history 230
  interface policy 31
  policy 287
  policy package 31, 224
  preview 128
  quick 32, 132, 235
  wizard 31, 224
interface
  configuring 87
  incoming 280
  outgoing 280
  policies 128
  single 35
interface list 86
intrusion protection 278, 443
  enable 445, 448
IP address
  NAT 456
  override 453
IP pools 280
IPS 350, 455
  inspection 280
  settings 449
IPsec VPN 280
IPv6 34
IPv6 static routes
  add 89
  configuring 89

J

javascript 75
JSON API 34

L

language 44, 106
  add 441
  delete 442
  edit 442
  report 424, 441
  Web-based Manager 44
layers 38
  transport 280
layout 32
LDAP server 46, 101
  add 101
  configuration 101
  delete 105
  modify 104
license
  FortiGuard 443
  information 72, 494
  list 494
  VM 491
lifecycle 38
lightweight directory access protocol. See LDAP
link
  VDOM 162
list
  device licenses 494
  FortiAP client 168
  rogue AP 169
lock
  ADOM 31, 56, 131, 284, 291
  ADOM revision 335
  override 31, 132
log 38, 64
  archive 370
  AV updates 459
  browse 371
  delete 126
  disable rolling 378
  download 374
  file size 126
  filters 392
  gzip 126
  import 373
  IPS updates 459
  messages 111
  rating queries 460
  receive monitor 76
  received 78
  roll 126, 375, 379
  rolling size 378
  rollover 126
  rotate 376
  rotation 376
  rotation settings 125
  service updates 450
  settings 114, 125, 376
  system events 125
  to disk 125, 376
  type 427
  updates 460
  upload 126, 375, 376, 377
  uploading 125
  view packets 370
  viewing 111
log array 165
  create new 165
  delete 166
  edit 166
log view 359
  column order 368
  columns 368
  customize 367
  details 369
  filter 369
logo 275

M

mail server 114, 439
  alerts 121
  create new 121
  delete 122, 123
  edit 122, 123
  settings 121
manage
  chassis 127, 171
  FortiGates 458
  objects 350
  packages 462
  queries 465
  VPN 54

management
centralized 37
firmware 37
lifecycle 38
management interface 85
administrative access 85
default gateway 86
IP address 85
IPv6 address 85
netmask 85
service access 86
map
dynamic object 354
zones 231
maximum
values 493
memory utilization 71
meta
fields 114, 123
metadata 114, 155
create new 124
delete 124, 125
edit 125
file format 156
MIB 118, 120
field 120, 121
RFC 1213 118, 119
RFC 2665 118, 119
mode
advanced 55
backup 54
device 55
discovery 209
normal 54
offline 127
model
device 208
modify
profile 100
monitor
administrator sessions 92
events 383
HA 473
HA status 477
task 113
more (CLI command) 255
move
element 420
widget 60

N

name
ADOM 53
chart 431
report 403
SNMP community 117
NAT 280
device 456
port 456
netmask
administrator account 96
network 85
cluster 476
configuration 476
diagnostic tools 86
DNS 86
interface list 86
interfaces 86, 87
IPv6 routing table 86
IPv6 static routing 89
management interface 85
routing table 86
static routing 88
network address translation. See NAT
network time protocol. See NTP
new
administrator 33
VDOM link 162
non-events 460
normal mode 54
NTP 64

O

objects 38, 278, 350
clone 356
create new 354
delete 356
drag and drop 350, 357
dynamic 350
edit 356
global 281
information 351
managing 350
map 354
remove 356
search 357
tool tip 351
where used 356
offline mode 127
organize
ADOMs 48
out-of-date 456
override
ADOM lock 132
FortiGuard server 452
server 450, 451, 453, 457

P

package 279, 282
deployed 463
global 281
history 464, 466
manage 462
query 466
received 462, 465
version 463
packet 279
action 280
packet log 370

password 67, 68
policy 106
paste
policy 331
PAT 280
peer list 472
PEM 173
view 174
perform
consistency check 290
policy check 290
platform type 62
policies 38, 278
actions 280
clone 330
consistency check 289
copy 331
create new 291
cut 331
delete 331
edit 330
footer 39
global 281
header 39
insert 330
install 224, 358
paste 331
quick install 235
reordering 159
sections 331
security 279, 299, 302
subtype 280
target 288
type 280
wizard 231
workflow 281
policy check
perform 290
results 290
policy folder
delete 286
rename 286
policy package
assign 286
create new 284
delete 286
export 288
global 284
install 287
installation targets 288
rename 286
polling
email filters 458
frequency 446
interval 458
POP3 280
populated data
drill down 380, 381, 382
port
forwarding 456
NAT 456
number 44
override 453
remote 118
settings 454
port address translation. See PAT
portal
profile 271
properties 275
power entry module. See PEM
PPPoE 456
preview
installation 128
private
FortiGuard servers 452
privileges 278
profile
add 179
administrator 98
client reputation 202
configure 32
configuring 99
create new 99, 439
delete 100, 179, 189, 194, 441
device 31, 131, 177
edit 179, 441
endpoint 196, 201
modify 100
output 439
package 98
portal 271
provisioning 131, 177
report 403
restricted 98
security 299, 302
standard 98
super 98
WIDS 191
wireless 131, 186
prompt 76
protocol
FGFM 50
provisioning
profiles 131, 177
services 37
proxy
intermediary 457
proxy server
IP address 456
port 456
push
enable 455, 456
scripts 50
update 446, 450, 455, 465

Q

query 461
  server 465
  status 466
quick install 32, 132, 235

R

RADIUS server 46, 103
  configuration 103
  create new 103
  delete 105
  modify 104
  secret 103
RAID
  configure 81
  management 26
  RAID 0 82
  RAID 10 83
  RAID 5 83
  RAID 5 +Spare 83
  RAID 50 83
  RAID 6 83
  RAID 6 +Spare 83
  RAID 60 83
  RAID linear 82
  RAID1 82
  supported levels 82
raw logs
  event details 384
reboot 47, 74
receive
  status 462, 465
red 453
redundant array of independent disks. See RAID
refresh
  device 152
remote
  authentication 101
  port 118
remove
  object 356
rename
  folder 286
  policy 286
reordering
  policies 159
replace
  managed device 148
report 38
  advanced settings 424
  break 417
  calendar 33, 434
  charts 33, 426
  configuration 33
  cover 411, 424
  datasets 434
  delete 425
  device list 424
  download 425
  edit 420
  export template 421
  filters 423
  heading 414
  historical 33
  history 33, 424
  import template 421
  language 404, 424, 441
  latest 424
  LDAP query 423
  name 403
  obfuscate names 424
  output 439
  per-device 403
  pre-defined 25
  profile 403, 439
  run 404, 405, 422
  schedule 404, 422, 423
  schedules 33
  section 408, 409
  table of contents 424
  templates 25, 33, 396, 397
  text 415
  time period 403
  type 403
  workspace 419
reputation 202
reset
  dashboard 61
resource limit
  configure 164
  VDOMs 163, 164
restore 67
  database 461
revision 37
  history 333
  lock 335
  unlock 335
RFC
  1213 118, 119
  1215 119
  2665 118, 119
rogue AP 169
roll
  log file 126
  logs 375, 378
routability 454
routing
  static 88, 89
  table 88, 89

run
report 404, 405, 422
schedule 422
script 244, 249

S

SAP 173, 176
schedule 64, 280
AV updates 458
create new 33
delete 422
disable 423
edit 422
IPS updates 458
polling 458
reports 33, 422
run 422
updates 446, 450, 458
web filtering 458
SCP
server 126
SCP server 376
script 34, 38, 50, 242, 243
clone 246
configure 243
create new 245
delete 247
edit 246
execute 244
execution history 248
export 247
history 249
import 248
re-run 249
run 244
Tcl scripts 256
troubleshooting tips 255
search
object 357
sections
add 331
secure shell. See SSH
security 37, 46
infrastructure 38
policies 279
serial number 62, 148
change 149
server
authentication 92
FortiAnalyzer 376
FQDN 123
FTP 126, 376
LDAP 101
mail 114, 439
override 450, 451, 453
RADIUS 103
remote authentication 101
SCP 126, 376
SFTP 126, 376
SMTP 121
syslog 114, 122, 123
TACACS+ 104
service status 464
services 37, 280, 350
set time 65
settings
administrator 105
advanced 114, 127
antivirus 449
columns 130
device log 114
install 224
IPS 449
log 376
log rotation 125, 376
logs 125
network 85
port 454
syslog server 122
severity
events 384
SFTP
server 126
SFTP server 376
shelf alarm panel. See SAP
shelf manager 173
shutdown 47, 74
simple network management protocol. See SNMP
SMTP server 121
SNMP 114, 115
agent 115
community 116
configure 115
configuring 115, 116
enable agent 116
manager 115, 120
MIB 120
MIBs 118
RFC 1213 118, 119
RFC 1215 119
RFC 2665 118, 119
system name 63
traps 119
v1 118
v2c 118

SNMP community
configuring 116
create new 116
name 117
source
address 280
IP address 280
spam 447, 460
special characters 64
SQL
query dataset 436
SSH 34, 45, 75, 454
SSID
clone 184
create new 179, 180
delete 179, 184
edit 184
import 179, 185
SSL 64
SSL-VPN 280
start
HA 472
static routes
add 88, 89
configuring 88
IPv6 89
statistics 79
status
FortiGuard 457
task 114
string
transliteration 156
supported web browsers 40
synchronize 30
device 127
HA 471
interval 65
syslog server 114
create new 122
events 393
name 123
settings 122
system
advanced settings 114
backup 66
checkpoint 68
firmware update 65
information 62
resources 70, 71
restore 67
settings 38, 114
template 177
time 62, 64, 65
system event
event management 393

T

TACACS+ server 46, 104
configuration 104
create new 104
delete 105
modify 104
task
delete 113
list size 127
monitor 113
status 114
TCP 375
port 443 454, 455
port 8890 454
Telnet 34, 75
template
add break 417
add chart 411
add headings 414
add image 413
add section 408, 409
add text 415
charts 426
clone 407
create new 406
endpoint 195
export 407, 421
folder 408
import 407, 421
report 396, 397
system 177
WiFi 179
workspace 419
threat activity
drill down 382
threat level 202
time 64
configure 64
report 403
set 65
system 65
zone 65
timeout 106
tool tip 351
traffic 271, 279
traffic activity
drill down 380
traffic log
event handler 389
transliteration
strings 156
transport layer 280
traps
Fortinet 118
SNMP 119
trusted host 46
security issues 97

U

UDP
  port 9443 456
unit
  backup 470
  fail 471
  operation 74
  primary 470
unlock
  ADOM 131
  ADOM revision 335
unregistered 455
  devices 158
update
  firmware 65, 480
  FortiAP 168
  histories 446
  history 464, 466
  logs 450, 460
  push 446, 465
  schedule 446, 450, 458
updates
  FortiManager 199
upgrade
  ADOM 51, 54
  HA cluster 478
upload
  enable 126, 376
  logs 125, 375, 376, 377
upload logs
  FortiAnalyzer 198
  FortiManager 198
uptime 63
up-to-date 458
usage
  CPU 71
  hard disk 71
  memory 71
US-ASCII 64
using
  web portal 277
UTM profile 280

V

VDOM 48, 271, 279
  add 219
  configuring 160
  creating 160
  enable 160
  global resources 164
  resource limit 163, 164
verify
  installation 128
version
  ADOM 24, 51, 80
  firmware 62
view
  event logs 384
  GB per day 73
  log messages 384
  logs 359
  managed devices 133
  object mappings 355
  packet log 370
  PEM 174
  SQL query 438
violation traffic 280
virtual domain. See VDOM
virtual IP 280
virus 460
VM
  licenses 491
VPN
  management 54

W

web
  proxy 446, 450, 452, 453, 456
web activity
  drill down 381
web browser
  supported 40
web filter 350, 443, 446, 449
  enable 446, 448
web portal 271
  add a logo 275
  add content 273
  add user 276
  design window 273
  external users 276
  properties 275
  using 277
web portal profile
  configuring 273
  create new 272
web services description language. See WSDL
Web-based Manager
  idle timeout 46
  language 44
  layout 32
weekly
  log rolling 379
where used 356
widget
  add 60
  alert message console 74
  CLI console 75
  license information 72
  log receive monitor 76
  logs/data received 78
  move 60
  options 61
  statistics 79
  system information 62
  system resources 70, 71
  unit operation 74

WIDS 139, 191
WIDS profile
clone 194
create new 191, 192
delete 191, 194
edit 194
import 191, 194
WiFi
templates 179
wireless intrusion detection system. See WIDS
wireless profile 131
clone 189
create new 186, 187
delete 186, 189
edit 189
import 186, 189
wizard
add device 206, 219
chart 426
import policy 231
install 31, 224
launching 207
workspaces 52, 131
enable 131
WSDL
file download 127

X

XML
API 34

Z

zone
bind 32
map 231
single interface 35