FortiAnalyzer v5.0 Patch Release 6
Administration Guide

FortiAnalyzer v5.0 Patch Release 6 Administration Guide

March 10, 2014

05-506-187572-20140310

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 **8**
Change Log **11**
Introduction **12**
FortiAnalyzer features 13
Scope 13
Entering FortiAnalyzer configuration data 14
Entering text strings (names) 14
Selecting options from a list 14
Enabling or disabling options 14
What's New in FortiAnalyzer v5.0 ..... **15**
FortiAnalyzer v5.0 Patch Release 6 15
Charts 15
Reports 15
Logging 15
Event management 15
Other 16
FortiAnalyzer v5.0 Patch Release 5 16
Cover page customization 16
Report text element customization 16
SIP/SCCP datasets 16
Summary of enhancements: 16
FortiAnalyzer v5.0 Patch Release 4 17
Chart builder wizard 17
System dashboard widgets 17
Report templates 17
Summary of enhancements: 18
FortiAnalyzer v5.0 Patch Release 3 18
RAID Management page 18
Pre-processing logic of ebtime 19
FortiMail/FortiWeb logging and reporting support 19
Drill Down tab 19
Event Management tab 20
FortiAnalyzer VM support for Microsoft Hyper-V Server 20
Import and export report templates 20
Summary of enhancements 20

FortiAnalyzer v5.0 Patch Release 2 21
Log arrays 21
FortiClient logging 22
Backup/restore logs and reports 22
Reliable FortiAnalyzer logging 22
Predefined charts and datasets for wireless 22
Web-based Manager enhancements 23
SNMP support and MIB updates 23
CLI command branch change 23
SQL query tool in the Web-based Manager 23
XML web service support 24
Summary of enhancements 24
FortiAnalyzer v5.0 Patch Release 1 25
Key Concepts 26
Administrative domains 26
Operation modes 26
Feature comparison between Analyzer and Collector mode 27
Analyzer mode 27
Analyzer and collector mode 28
Log storage 29
Workflow 30
Web-based Manager 31
System requirements 31
Web browser support 31
Screen resolution 31
Connecting to the Web-based Manager 32
Web-based Manager overview 32
Web-based Manager configuration 34
Language support 34
Administrative access 35
Restricting access by trusted hosts 36
Idle timeout 36
Reboot and shutdown the FortiAnalyzer unit 37
Administrative Domains 38
Adding an ADOM 39
Assigning devices to an ADOM 41
Assigning administrators to an ADOM 41
ADOM device modes 42
Device Manager 43
Devices 45
Devices and VDOMs 45
Unregistered devices 51

Log arrays 51
Device reports 54
Log forwarding 54
System Settings 56
Dashboard 57
Customizing the dashboard 59
System Information widget 60
License Information widget 66
Unit Operation widget 67
System Resources widget 68
Alert Messages Console widget 70
CLI Console widget 71
Statistics widget 72
Logs/Data Received widget 72
Log Receive Monitor widget 73
All ADOMs 75
RAID Management 77
Supported RAID levels 79
RAID disk status 82
Hot swapping hard disks 82
Adding new disks 83
Network 84
Network interfaces 85
Static routes 87
IPv6 static routes 88
Diagnostic tools 89
Admin 89
Monitoring administrator sessions 90
Administrator 91
Profile 95
Remote authentication server 99
Administrator settings 104
Certificates 105
Local certificates 105
CA certificates 108
Certificate revocation lists 109
Event log 110
Task monitor 112

Advanced 113
SNMP v1/v2c 113
Mail server 118
Syslog server 118
Meta fields 119
Device log settings 121
File management 122
Advanced settings 123
Drill Down 124
Traffic 124
Web activity 125
Email activity 125
Threat 126
Event Management 127
Events 127
Event details 129
Acknowledge events 130
Event handler 131
Manage event handlers 134
Log View 137
Viewing log messages 138
Customizing the log view 139
Searching log messages 142
Download log messages 144
Log details 145
Archive 145
Browsing log files 146
Importing a log file 148
Downloading a log file 149
FortiClient logs 149
Configuring rolling and uploading of logs 150
Reports 153
Reports 154
Default reports 156
Configure reports 161
Run a report 162
Schedules 163
Advanced settings 163
Completed reports 165

Report templates 166
Workspace settings 167
Sections 168
Elements 170
Import and export 176
Report cover pages 176
Chart library 178
Custom chart wizard 179
Managing charts 183
Report calendar 186
Advanced 187
Dataset 187
Output profile 191
Language 193
FortiAnalyzer Firmware 195
Upgrading from FortiAnalyzer v5.0 Patch Release 5 195
Upgrading from FortiAnalyzer v4.0 MR3 195
General firmware upgrade steps 196
Downgrading to previous versions 199
Appendix A: SNMP MIB Support 200
Appendix B: Port Numbers 201
Appendix C: Maximum Values Matrix 203
Maximum values matrix 203
Appendix D: FortiAnalyzer VM 205
Licensing 205
FortiAnalyzer VM firmware 206
Appendix E: MySQL databases 207
Setting up FortiAnalyzer with an external MySQL database 207
Index 209

Table of Figures

Figure 1: RAID management page 19
Figure 2: Create log array dialog box 21
Figure 3: System resources widget 23
Figure 4: Edit dataset dialog box 23
Figure 5: Download WSDL file dialog box 24
Figure 6: Topology of the FortiAnalyzer unit in analyzer mode 27
Figure 7: Topology of the FortiAnalyzer units in analyzer/collector mode 28
Figure 8: Logging, analyzing, and reporting workflow 30
Figure 9: The tab bar 33
Figure 10: Administration settings 34
Figure 11: Network management interface 36
Figure 12: Unit operation actions in the Web-based Manager 37
Figure 13: Create an ADOM 39
Figure 14: Edit an ADOM 40
Figure 15: Device Manager tab 43
Figure 16: Column right-click menu 44
Figure 17: Add device wizard login screen 45
Figure 18: Add device wizard add device screen 46
Figure 19: Add device wizard add device screen two 47
Figure 20: Add device wizard summary screen 48
Figure 21: Edit a device 49
Figure 22: Unregistered device dialog box 51
Figure 23: Promote unregistered devices 51
Figure 24: Create log array window 52
Figure 25: Rebuild log array dialog box 53
Figure 26: Rebuild log array dialog box. 53
Figure 27: Add log forwarding dialog box 55
Figure 28: FortiAnalyzer system settings dashboard 57
Figure 29: Click an active module name to add module to page dialog box 59
Figure 30: A minimized widget 59
Figure 31: System information widget 60
Figure 32: Change host name dialog box 62
Figure 33: Change system time settings dialog box 63
Figure 34: Backup dialog box 64
Figure 35: Restore dialog box 65
Figure 36: Change operation mode 66
Figure 37: License information widget 66
Figure 38: VM License information widget 67
Figure 39: Unit operation widget 67
Figure 40: System resources widget (real time display) 68
Figure 41: System resources widget (historical display) 68
Figure 42: Edit system resources settings window 69
Figure 43: Alert message console widget 70
Figure 44: List of all alert messages 70
Figure 45: CLI console widget 71
Figure 46: Statistics widget 72
Figure 47: Logs/data received widget (real-time) 72

Figure 48: Logs/data received widget (historical) 72
Figure 49: Edit logs/data received settings window 73
Figure 50: Log receive monitor widget (log type) 73
Figure 51: Edit log receive monitor settings 74
Figure 52: All ADOMs list 75
Figure 53: Create a new ADOM 76
Figure 54: RAID Management menu page 78
Figure 55: RAID settings dialog box 78
Figure 56: Network page 84
Figure 57: Network interface list 85
Figure 58: Configure network interfaces 86
Figure 59: Routing table 87
Figure 60: Create new route 87
Figure 61: IPv6 routing table 88
Figure 62: Create new route 88
Figure 63: Diagnostic tools 89
Figure 64: Example Ping diagnostics output 89
Figure 65: Administrator session list 90
Figure 66: Administrator list 91
Figure 67: New administrator dialog box 92
Figure 68: Edit administrator page 94
Figure 69: Administrator profile list 97
Figure 70: Create new administrator profile 98
Figure 71: Server list 99
Figure 72: New LDAP server dialog box 101
Figure 73: New RADIUS Server window 102
Figure 74: New TACACS+ server dialog box 103
Figure 75: Settings dialog box 104
Figure 76: Local certificates sub-menu 105
Figure 77: New local certificate 106
Figure 78: Result page 107
Figure 79: Result page 108
Figure 80: Local log list 110
Figure 81: Task monitor window 112
Figure 82: SNMP v1/v2c dialog box 114
Figure 83: New SNMP community 116
Figure 84: Mail server window 118
Figure 85: Mail server settings 118
Figure 86: Syslog server window 119
Figure 87: Syslog server settings 119
Figure 88: System metadata 119
Figure 89: Add a meta-field 120
Figure 90: Device log settings window 121
Figure 91: File Management 122
Figure 92: Example WSDL file 123
Figure 93: Drill Down tab and data 124
Figure 94: Events page 127
Figure 95: Event details page 129
Figure 96: Event handler page 133
Figure 97: Create new event handler page 134
Figure 98: Log view 138
Figure 99: Raw logs 140

Figure 100: Column settings 140
Figure 101: Filter settings 141
Figure 102: Search history 142
Figure 103: Custom timeframe 142
Figure 104: Bookmarks 143
Figure 105: Example searches 144
Figure 106: Download log messages 144
Figure 107: Log details 145
Figure 108: Log archive 145
Figure 109: View packet log 146
Figure 110: Log file list window 147
Figure 111: Import log file dialog box 148
Figure 112: Download log file dialog box 149
Figure 113: FortiClient logs 149
Figure 114: Report page 154
Figure 115: Create report page 161
Figure 116: Schedule a report template 163
Figure 117: Advanced report settings 163
Figure 118: Report filters 164
Figure 119: Completed reports 165
Figure 120: Device reports 166
Figure 121: Default new report template 166
Figure 122: Edit workspace 167
Figure 123: Section toolbar 168
Figure 124: Add a new section 169
Figure 125: Template toolbar 170
Figure 126: Edit heading dialog box 171
Figure 127: Edit text dialog box 172
Figure 128: Choose a graphic dialog box 173
Figure 129: Add a new chart 174
Figure 130: Chart filters 175
Figure 131: Edit predefined chart 175
Figure 132: Cover page settings 176
Figure 133: Chart library 178
Figure 134: Choose data 179
Figure 135: Add filters page 180
Figure 136: Preview page 182
Figure 137: Create new chart 183
Figure 138: Report calendar 186
Figure 139: Datasets 188
Figure 140: Create a new dataset 189
Figure 141: Edit a dataset 190
Figure 142: SQL query pop-up window 191
Figure 143: Output profile page 191
Figure 144: Create new output profile dialog box 192
Figure 145: Report language 193
Figure 146: Create a new language 194
Figure 147: Firmware image checksums page 196
Figure 148: Backup dialog box 197
Figure 149: Snapshot of FortiAnalyzer VM (VMware) 198
Figure 150: Snapshot of FortiAnalyzer VM (Microsoft Hyper-V) 198

Change Log

Date	Change Description
2012-11-20	Initial release.
2013-01-14	Provisional document update for v5.0 Patch Release 1.
2013-04-02	Provisional document update for v5.0 Patch Release 2.
2013-04-24	Updated log rolling and uploading configuration and firmware update instructions.
2013-05-29	Updated introductory feature list.
2013-07-16	Provisional document update for v5.0 Patch Release 3.
2013-09-13	Provisional document update for v5.0 Patch Release 4.
2013-09-20	Added information on device disk log quota and log array disk log quota.
2013-11-13	Provisional document update for v5.0 Patch Release 5.
2014-01-30	Provisional document update for v5.0 Patch Release 6.
2014-02-24	Corrected typographic issues.
2014-03-10	Removed FortiAnalyzer supported devices from Introduction chapter. For more information, see the product datasheet.

Introduction

FortiAnalyzer platforms integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout your network. The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine-tune your policies. Organizations of any size will benefit from centralized security event logging, forensic research, reporting, content archiving, data mining and malicious file quarantining.

FortiAnalyzer offers enterprise class features to identify threats, while providing the flexibility to evolve along with your ever-changing network. FortiAnalyzer can generate highly customized reports for your business requirements, while aggregating logs in a hierarchical, tiered logging topology.

You can deploy FortiAnalyzer physical or virtual appliances to collect, correlate, and analyze geographically and chronologically diverse security data. Aggregate alerts and log information from Fortinet appliances and third-party devices in a single location, providing a simplified, consolidated view of your security posture. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches.

This is a provisional document.

This guide contains the following chapters and appendices:

- What's New in FortiAnalyzer v5.0
- Key Concepts
- Web-based Manager
- Administrative Domains
- Device Manager
- System Settings
- Drill Down
- Event Management
- Log View
- Reports
- FortiAnalyzer Firmware
- SNMP MIB Support
- Port Numbers
- Maximum Values Matrix
- FortiAnalyzer VM
- MySQL databases

FortiAnalyzer features

- Pre-defined and customized charts help you monitor and identify attack patterns, maintain acceptable use policies, and demonstrate policy compliance
- Network capacity and utilization data reporting allow you to plan and manage networks more efficiently
- Scalable architecture allows the FortiAnalyzer to run in collector or analyzer modes for optimized log processing
- Advanced features such as event correlation, forensic analysis, and vulnerability assessment provide essential tools for in-depth protection of complex networks
- Secure data aggregation from multiple FortiGate and FortiCarrier security appliances provides network-wide visibility and compliance
- Fully integrated with FortiManager appliances for a single point of command, control, analysis, and reporting
- Granular alert rules allow you to notify key personnel when specific events or triggers occur
- Reconcile various log types (such as traffic, web filter, and attack) to perform forensics with detailed logging capabilities
- Create custom SQL datasets, charts, and reports that can be imported and exported to other administrative domains or FortiAnalyzer units
- Deploy with either a physical hardware appliance or virtual machine (VMware ESX, ESXi and Microsoft Hyper-V) with multiple options to dynamically increase storage
- Event Management: Raise and monitor important events to present the IT administrator with unprecedented insight into potentially anomalous behavior
- Drill-downs: Generate ad-hoc graphical views of summary traffic, web, email and threat activity.

Scope

This document describes how to use the Web-based Manager to set up and configure a FortiAnalyzer unit. It assumes you have already successfully installed the FortiAnalyzer unit by following the instructions in your unit's QuickStart guide.

At this stage:

- You have administrative access to the Web-based Manager and/or Command Line Interface (CLI), and
- The FortiAnalyzer unit can connect to the Web-based Manager and CLI.

This document explains how to use the Web-based Manager to:

- Maintain the FortiAnalyzer unit, including backups
- Configure basic settings, such as system time, DNS settings, administrator passwords, and network interfaces
- Configure advanced features, such as adding devices, DLP archiving, logging, and reporting.

This document does not cover commands for the command line interface (CLI). For information on the CLI, see the *FortiAnalyzer v5.0 CLI Reference*.

Entering FortiAnalyzer configuration data

The configuration of a FortiAnalyzer unit is stored as a series of configuration settings in the FortiAnalyzer configuration database. Use the Web-based Manager or CLI to add, delete or change configuration settings. These configuration changes are stored in the configuration database as they are made.

Individual settings in the configuration database can be text strings, numeric values, selections from a list of allowed options, or on/off (enable/disable).

Entering text strings (names)

Text strings are used to name entities in the configuration. For example, the name of a report chart, administrative user, and so on. You can enter any character in a FortiAnalyzer configuration text string except, to prevent Cross-Site Scripting (XSS) vulnerabilities, the following characters:

" (double quote), & (ampersand), ' (single quote), < (less than), and > (greater than)

Selecting options from a list

If a configuration field can only contain one of a number of selected options, the Web-based Manager and CLI present you a list of acceptable options and you can select one from the list. No other input is allowed. From the CLI, you must spell the selection name correctly.

Enabling or disabling options

If a configuration field can only be on or off (enabled or disabled), the Web-based Manager shows a check box or other control that can only be enabled or disabled. From the CLI, you can set the option to `enable` or `disable`.

What's New in FortiAnalyzer v5.0

FortiAnalyzer v5.0 Patch Release 6

FortiAnalyzer v5.0 Patch Release 6 includes the following new features and enhancements. Always review all sections in the *FortiAnalyzer Release Notes* prior to upgrading your device.

Charts

- Chart improvements:
  - Charts in the *Chart Library* are listed in alphabetical order by default.
  - Charts have been renamed for improved usability.
  - The chart library and database have been improved.
- New charts
  - Botnet activity charts

    Four new charts have been added for Botnet activity.
  - Site-to-Site VPN charts.

See "Chart library" on page 178 for more information.

Reports

The following reports have been improved:

- Bandwidth and Applications Report
- Security Analysis report
- Threat Report
- User Report
- Web Usage Report

See "Reports" on page 154 for more information.

Logging

- Improved FortiAnalyzer insert rate performance
- Log filter improvements
- When the FortiAnalyzer device is in collector mode, you can configure log forwarding in the *Device Manager* tab. For more information, see "Log forwarding" on page 54.

Event management

- FortiOS v4.0 MR3 logs are now supported.
- Support subject customization of alert email.

See "Event Management" on page 127 for more information.

Other

- Automatically delete log files, quarantined files, reports, and content archive files older than a specified time period. For more information, see “File management” on page 122.
- FortiAnalyzer VM supports up to 12 virtual disks (LVM).

FortiAnalyzer v5.0 Patch Release 5

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

Cover page customization

You can now customize the report cover page images and text in the report template page.

See “Report cover pages” on page 176 for more information.

Report text element customization

You can now customize the report text element. You can apply bold and italics to text, indent text, and create both bulleted and numbered lists.

See “Text boxes” on page 172 for more information.

SIP/SCCP datasets

The following datasets have been added to FortiAnalyzer for SIP and SCCP support:

- appctrl-Top-Block-SCCP-Callers
- appctrl-Top-Blocked-SCCP-Callers-by-Blocking-Criteria
- content-Count-Total-SCCP-Call-Registrations-by-Hour-of-Day
- content-Count-Total-SCCP-Calls-Duration-by-Hour-of-Day
- content-Count-Total-SCCP-Calls-per-Status
- appctrl-Top-Blocked-SIP-Callers
- appctrl-Top-Blocked-SIP-Callers-by-Blocking-Criteria
- content-Count-Total-SIP-Call-Registrations-by-Hour-of-Day
- content-Count-Total-SIP-Calls-per-Status
- content-Dist-Total-SIP-Calls-by-Duration

Summary of enhancements:

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

Reports

- SIP/SCCP datasets
- Added Spyware, Adware, and other predefined charts to the Threat Report
- Added an OR option to the report filter
- Cover page customization
- Reorganize the configuration page layout for Schedule

Logging

- Added support to upload logs to multiple rolling servers
- Configurable FortiAnalyzer option and device filters for Log Forwarding and Aggregation
- Log Search enhancements

Other

- Added System Charts and Custom Charts checkboxes to filter out predefined charts or customized charts.
- Download FortiGuard Databases for more detailed reports
- Web-based Manager enhancement when rebuilding a log array

FortiAnalyzer v5.0 Patch Release 4

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

Chart builder wizard

A chart builder wizard has been added to allow you to create custom charts. See "Custom chart wizard" on page 179 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 72, "Logs/Data Received widget" on page 72, and "Log Receive Monitor widget" on page 73 for more information.

Report templates

FortiAnalyzer 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

Summary of enhancements:

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

Reports

- Option to remove the FortiAnalyzer report cover page
- Generate per user reports (setup via XML)
- Chart builder wizard
- Predefined report template for custom application report
- Predefined 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
- Report templates

Logging

- Log forward in CEF format
- 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
- System dashboard widgets

FortiAnalyzer v5.0 Patch Release 3

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

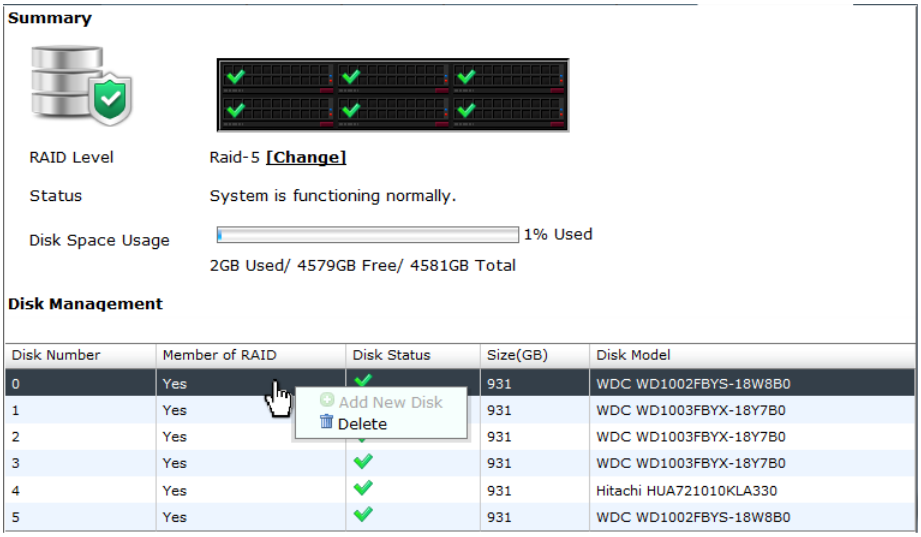
RAID Management page

A RAID Management menu item replaces the existing 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.

Figure 1: RAID management page



Pre-processing logic of ebtime

Logs with the following conditions met are considered usable for the calculation of estimated browsing time:

Traffic logs with `logid` of `13` or `2`, when `logid == 13`, `hostname` must not be empty. The `service` field should be either `HTTP`, `80/TCP` or `443/TCP`.

If all above conditions are met, then `devid`, `vdom`, and `user` (`srcip` if `user` is empty) are combined as a key to identify a user. For time estimation, the current value of `duration` is calculated against history session start and end time, only un-overlapped part are used as the `ebtime` of the current log.

FortiMail/FortiWeb logging and reporting support

FortiAnalyzer v5.0 Patch Release 3 or later supports FortiMail and FortiWeb logging and reporting. ADOMs must be enabled on FortiAnalyzer before these devices can be added. FortiMail and FortiWeb are log triggered devices. Once configured to log to the FortiAnalyzer 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 added using the Add Model Device wizard.

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.

FortiAnalyzer VM support for Microsoft Hyper-V Server

FortiAnalyzer VM now supports Microsoft Hyper-V Server 2008 R2 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 FortiAnalyzer device can be exported and imported into another FortiAnalyzer device.

Summary of enhancements

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

- Log search
- Device storage and log management
- RAID Management page
- Report Web-based Manager enhancements
- Merge event log based charts to the default report
- Chart level filters
- Report filter improvements
- Drill Down tab
- Event Management tab
- FortiMail logging and reporting support
- FortiWeb logging and reporting support
- FortiAnalyzer VM support for Microsoft Hyper-V Server
- Added support for real-time syslog forwarding over TCP connections
- Web Filter report template
- WiFi Network Summary report template
- Import and export report templates

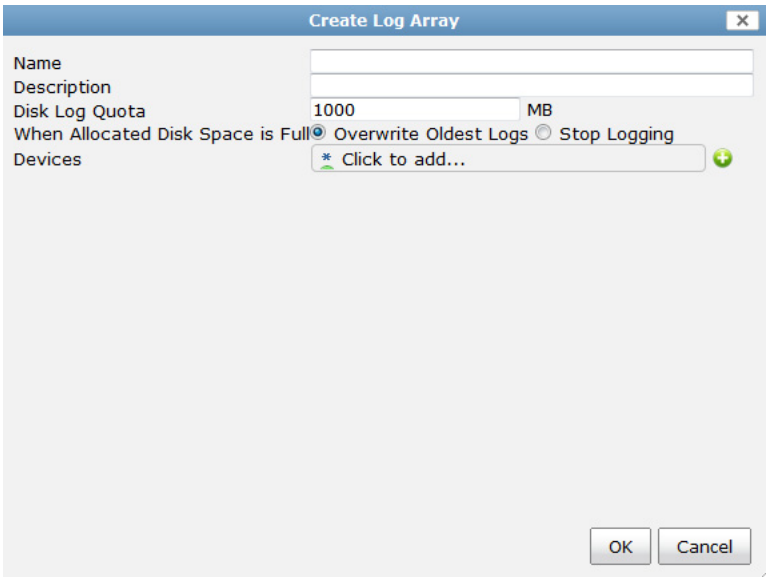
FortiAnalyzer v5.0 Patch Release 2

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

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. Log arrays also allow you to manage log data belonging to FortiGate high availability (HA) clusters from a single device object. You can add VDOMs from a single device to different log arrays. You can configure and schedule reports for each log array.

Figure 2: Create log array dialog box



Both the device disk log quota and the log array disk log quota are enforced. The device disk log quota includes all log files, all archive files, and database space for logs on the device. The log array disk log quota includes database space used by log array tables. The device disk log quota no longer applies when it is added to a 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 FortiAnalyzer device.

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

FortiClient logging

Support has been added to FortiAnalyzer to allow you to log FortiClient endpoint traffic. FortiClient logs are stored under a single device object. This feature requires FortiClient v5.0 Patch Release 2 or later.

Backup/restore logs and reports

The following CLI commands have been added to FortiAnalyzer v5.0 Patch Release 2 to allow you to backup and restore logs and reports:

- `execute backup logs`: Backup device logs to a specified server.
- `execute backup logs-only`: Backup device logs only to a specified server.
- `execute backup reports`: Backup reports to a specified server.
- `execute restore logs`: Restore device logs and DLP archives from a specified server.
- `execute restore logs-only`: Restore device logs from a specified server.
- `execute restore reports`: Restore reports from a specified server.

Reliable FortiAnalyzer logging

FortiAnalyzer v5.0 Patch Release 2 or later supports reliable logging.

Predefined charts and datasets for wireless

The following charts and datasets have been added for wireless support:

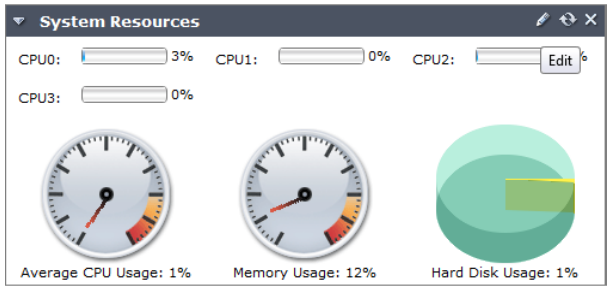
- chart: "default-AP-Detection-Summary-by-Status-OnWire"
  dataset: "default-AP-Detection-Summary-by-Status-OnWire"
- chart: "default-AP-Detection-Summary-by-Status-OffWire"
  dataset: "default-AP-Detection-Summary-by-Status-OffWire"
- chart: "default-AP-Detection-Summary-by-Status-OnWire_Table"
  dataset: "default-AP-Detection-Summary-by-Status-OnWire"
- chart: "default-AP-Detection-Summary-by-Status-OffWire_Table"
  dataset "default-AP-Detection-Summary-by-Status-OffWire"
- chart: "default-selected-AP-Details-OnWire"
  dataset "default-selected-AP-Details-OnWire"
- chart: "default-selected-AP-Details-OffWire"
  dataset: "default-selected-AP-Details-OffWire"
- chart: "default-Managed-AP-Summary"
  dataset: "default-Managed-AP-Summary"
- chart: "default-Managed-AP-Summary_Table"
  dataset: "default-Managed-AP-Summary"
- chart: "event-Wireless-Client-Details"
  dataset: "event-Wireless-Client-Details"

Web-based Manager enhancements

System Resources widget

The System Resources widget displays CPU usage for each processor core, and memory and hard disk usage information. See "System Resources widget" on page 68 for more information.

Figure 3: System resources widget



SNMP support and MIB updates

FortiAnalyzer v5.0 Patch Release 2 enhances SNMP support and Management Information Bases (MIBs) have been updated.

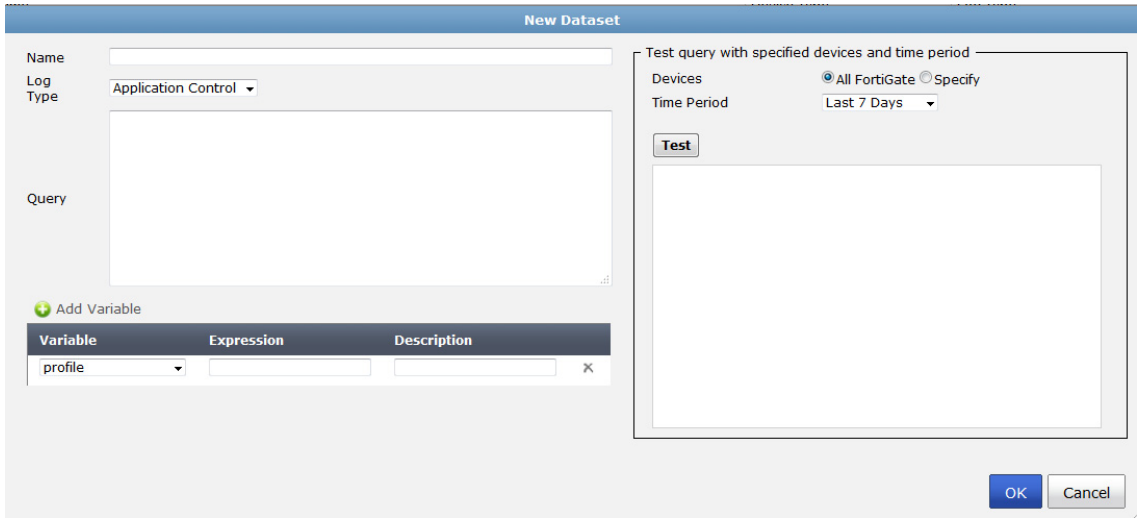
CLI command branch change

In FortiAnalyzer v5.0 Patch Release 2, the `fmsystem` and `fasystem` CLI branches have been merged into the `system` branch.

SQL query tool in the Web-based Manager

An SQL query tool has been added to the Web-based Manager to allow you to test SQL datasets. After you choose a log type and set up variables for the filter you can test the SQL query before saving the setting.

Figure 4: Edit dataset dialog box



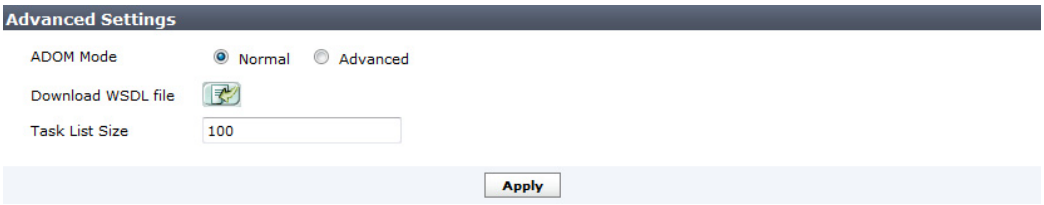
XML web service support

FortiAnalyzer web services has been enhanced to support SQL reporting. The following APIs are now supported in SQL:

- runFazReport
- getFazGeneratedReport
- listFazGeneratedReports
- getFazArchive
- removeFazArchive
- getSystemStatus
- getFazConfig
- setFazConfig
- searchFazLog

To download the Web Server Description Language (WSDL) file on your FortiAnalyzer, go to *System Settings* > *Advanced* > *Advanced Settings*. Select the download WSDL file icon to save the file to your management computer.

Figure 5: Download WSDL file dialog box



Summary of enhancements

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

- Log arrays
- Group reports
- Backup/restore logs and reports
- CLI command branch change
- Client reputation report template
- FortiClient logging
- Predefined charts and datasets for wireless
- Reliable FortiAnalyzer logging
- Report template updates
- SNMP support and MIB updates
- SSQL query tool in the Web-based Manager
- *System Resources* widget enhancement
- XML web service support

FortiAnalyzer v5.0 Patch Release 1

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

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

- Added support for IPv6 networking
- Auto-generate log fields
- Certificate compatibility with FortiGate
- Dataset improvements
- Device Manager
- FortiOS v5.0.0 support
- GTP log compatibility
- Improved Collector and Analyzer modes
- Log Aggregation (Collector mode)
- Multiple concurrent running reports
- New DVM table
- New FortiAnalyzer VM licensing model
- New PDF report style
- Removed index-based logging and reporting
- Support OU for the report LDAP filter
- Support upgrade from FortiAnalyzer v4.0 MR3

Key Concepts

This chapter defines basic FortiAnalyzer concepts and terms.

If you are new to FortiAnalyzer, this chapter can help you to quickly understand this document and your FortiAnalyzer platform.

This topic includes:

- Administrative domains
- Operation modes
- Log storage
- Workflow

Administrative domains

Administrative domains (ADOMs) enable the `admin` administrator to constrain other FortiAnalyzer unit administrators' access privileges to a subset of devices in the device list. For Fortinet devices with virtual domains (VDOMs), ADOMs can further restrict access to only data from a specific device's VDOM.

Enabling ADOMs alters the structure of and the available functions in the Web-based Manager and CLI, according to whether or not you are logging in as the `admin` administrator, and, if you are not logging in as the `admin` administrator, the administrator account's assigned access profile. See "System Information widget" on page 60 for information on enabling and disabling ADOMs.

For information on working with ADOMs, see "Administrative Domains" on page 38. For information on configuring administrators and administrator settings, see"Admin" on page 89.

ADOMs must be enabled to support FortiCarrier, FortiMail and FortiWeb logging and reporting. See "To enable the ADOM feature:" on page 38.

Operation modes

The FortiAnalyzer unit has two operation modes:

- *Analyzer*: The default mode that supports all FortiAnalyzer features. This mode used for aggregating logs from one or more log collectors. In this mode, the log aggregation configuration function is disabled.
- *Collector*: The mode used for saving and uploading logs. For example, instead of writing logs to the database, the collector can retain the logs in their original (binary) format for uploading. In this mode, the report function and some functions under the System Settings tab are disabled.

The analyzer and collector modes are used together to increase the analyzer's performance. The collector provides a buffer to the FortiAnalyzer by off-loading the log receiving task from the analyzer. Since log collection from the connected devices is the dedicated task of the collector, its log receiving rate and speed are maximized.

The mode of operation that you choose will depend on your network topology and individual requirements. For information on how to select an operation mode, see “Changing the operation mode” on page 65.

Feature comparison between Analyzer and Collector mode

In FortiAnalyzer v5.0 Patch Release 6, the operation mode options have been simplified to two modes, Analyzer and Collector. Standalone mode has been removed.

Table 1: Feature comparison between Analyzer and Collector modes

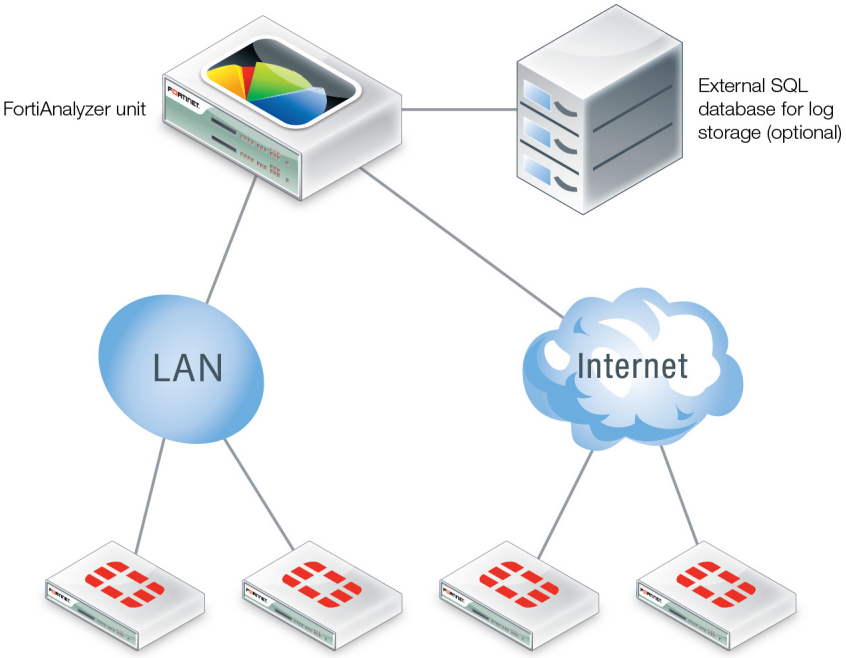
	Analyzer Mode	Collector Mode
Event Management	✔	
Monitoring (drill-down/charts)	✔	
Reporting	✔	
Log View	✔	✔
Device Manager	✔	✔
System Settings	✔	✔
Log Forwarding		✔

Analyzer mode

The analyzer mode is the default mode that supports all FortiAnalyzer features. If your network log volume does not compromise the performance of your FortiAnalyzer unit, you can choose this mode.

Figure 6 illustrates the network topology of the FortiAnalyzer unit in analyzer mode.

Figure 6: Topology of the FortiAnalyzer unit in analyzer mode



Monitored devices that send logs to the FortiAnalyzer unit for analyzing and reporting.

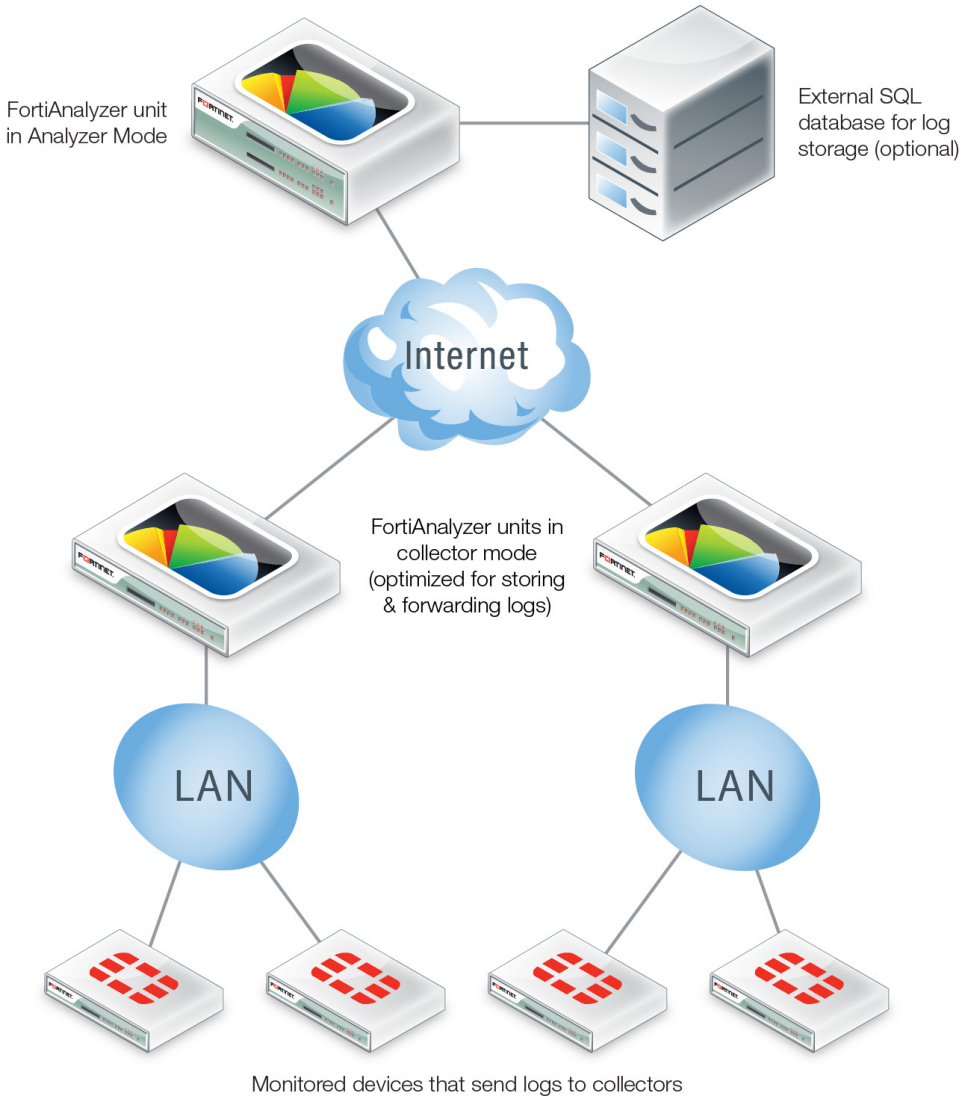
Analyzer and collector mode

The analyzer and collector modes are used together to increase the analyzer's performance. The collector provides a buffer to the analyzer by off-loading the log receiving task from the analyzer. Since log collection from the connected devices is the dedicated task of the collector, its log receiving rate and speed are maximized.

In most cases, the volume of logs fluctuates dramatically during a day or week. You can deploy a collector to receive and store logs during the high traffic periods and transfer them to the analyzer during the low traffic periods. As a result, the performance of the analyzer is guaranteed as it will only deal with log insertion and reporting when the log transfer process is over.

As illustrated in Figure 7: company A has two remote branch networks protected by multiple FortiGate units. The networks generate large volumes of logs which fluctuate significantly during a day. It used to have a FortiAnalyzer 4000B in analyzer mode to collect logs from the FortiGate units and generate reports. To further boost the performance of the FortiAnalyzer 4000B, the company deploys a FortiAnalyzer 400C in collector mode in each branch to receive logs from the FortiGate units during the high traffic period and transfer bulk logs to the FortiAnalyzer 4000B during the low traffic period.

Figure 7: Topology of the FortiAnalyzer units in analyzer/collector mode



To set up the analyzer/collector configuration:

1. On the FortiAnalyzer unit, go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Operation Mode* field, select *Change*.
3. Select *Analyzer* in the *Change Operation Mode* dialog box.
4. Select *OK*.
5. On the first collector unit, go to *System Settings* > *Dashboard.*
6. In the *System Information* widget, in the *Operation Mode* field, select *Change*.
7. Select *Collector* the *Change Operation Mode* dialog box.
8. Select *OK*.

   For more information on configuring log forwarding, see “Log forwarding” on page 54.

Log storage

The FortiAnalyzer unit supports Structured Query Language (SQL) logging and reporting. The log data is inserted into the SQL database for generating reports. Both local and remote SQL database options are supported.

For more information, see “Reports” on page 153.

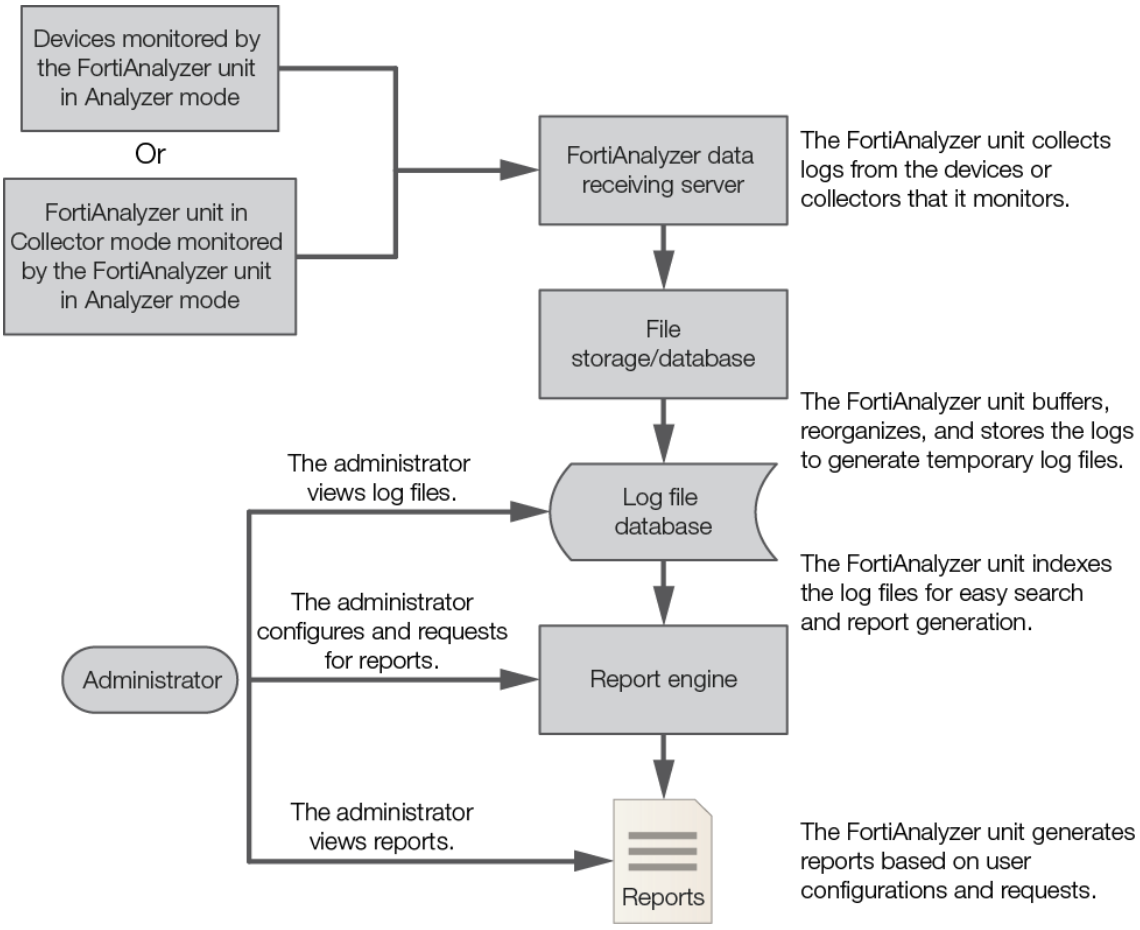
Workflow

Once you have successfully deployed the FortiAnalyzer platform in your network, using and maintaining your FortiAnalyzer unit involves the following:

- Configuration of optional features, and re-configuration of required features if required by changes to your network
- Backups
- Updates
- Monitoring reports, logs, and alerts

Figure 8 illustrates the process of data logging, data analyzing, and report generation by the FortiAnalyzer unit in analyzer mode.

Figure 8: Logging, analyzing, and reporting workflow



Web-based Manager

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

This section includes the following topics:

- System requirements
- Connecting to the Web-based Manager
- Web-based Manager overview
- Web-based Manager configuration
- Reboot and shutdown the FortiAnalyzer unit

Additional configuration options and short-cuts are sometimes available through right-click menus. Right-clicking the mouse in various location in the interface accesses these options.

System requirements

Web browser support

The FortiAnalyzer Web-based Manager supports the following web browsers:

- Microsoft Internet Explorer versions 10 and 11
- Mozilla Firefox version 27
- Google Chrome version 32

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

Screen resolution

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

Please refer to the *FortiAnalyzer Release Notes* for product integration and support information.

Connecting to the Web-based Manager

The FortiAnalyzer 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.

For more information on connecting your specific FortiAnalyzer unit, read that device's QuickStart Guide.

To connect to the Web-based Manager:

1. Connect the unit to a management computer using an Ethernet cable.
2. Configure the management computer to be on the same subnet as the internal interface of the FortiAnalyzer unit:
   - IP address: 192.168.1.2
   - Netmask: 255.255.255.0.
3. On the management computer, start a supported web browser and browse to `https://192.168.1.99`.
4. Type `admin` in the *User Name* field, leave the *Password* field blank, and select *Login*.

   You should now be able to use the FortiAnalyzer Web-based Manager.

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 86.

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 "Static routes" on page 87.

Web-based Manager overview

The FortiAnalyzer Web-based Manager consists of four primary parts: the tab bar, the main menu bar, the tree menu, and the content pane. The content pane includes a toolbar and, on some tabs, is horizontally split into two sections. The main menu bar is only visible on certain tabs when ADOMs are disabled (see "System Information widget" on page 60).

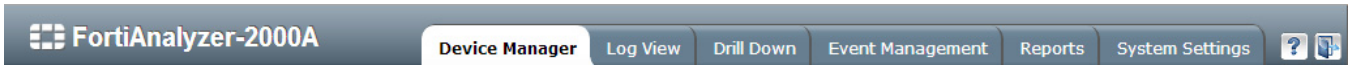
You can use the Web-based Manager menus, lists, and configuration pages to configure most FortiAnalyzer settings. Configuration changes made using the Web-based Manager take effect immediately without resetting the FortiAnalyzer system or interrupting service.

The Web-based Manager also includes online help, accessed by selecting the help icon,  , on right side of the tab bar.

Tab bar

The Web-based Manager tab bar contains the device model, the available tabs, the *Help* button, and the *Log Out* button.

Figure 9: The tab bar



Device Manager	Manage groups, devices, and VDOMs, and view real-time monitor data. For more information, see "Device Manager" on page 43.
Log View	View and download logs for connected devices. For more information, see "Log View" on page 137.
Drill Down	Drill down traffic, web, email, and threat activity for FortiGate, VDOMs, and log arrays. For more information, see "Drill Down" on page 124.
Event Management	Configure and view events for managed log devices. For more information, see "Event Management" on page 127.
Reports	Configure report templates, schedules, and output profiles, and manage charts and datasets. For more information, see "Reports" on page 153.
System Settings	Configure system settings such as network interfaces, administrators, system time, server settings, and others. You can also perform maintenance and firmware operations. For more information, see "System Settings" on page 56.
Help	Open the FortiAnalyzer online help.
Log Out	Log out of the Web-based Manager.

Tree menu

The Web-based Manager tree menu is on the left side of the window. The content in the menu varies depending on which tab is selected and how your FortiAnalyzer unit is configured. If ADOMs are enabled, the contents of the tree menu on all tabs, except the System Settings tab, will be organized by ADOM.

Some elements in the tree menu can be right-clicked to access different configuration options.

Content pane

The content pane is on the right side of the window. The information changes depending on which tab is being viewed and what element is selected in the tree menu. The content pane of the Device Manager, Log View, and Reports tabs is split horizontally into two frames.

Web-based Manager configuration

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

This section includes the following topics:

- Language support
- Administrative access
- Restricting access by trusted hosts
- Idle timeout

Language support

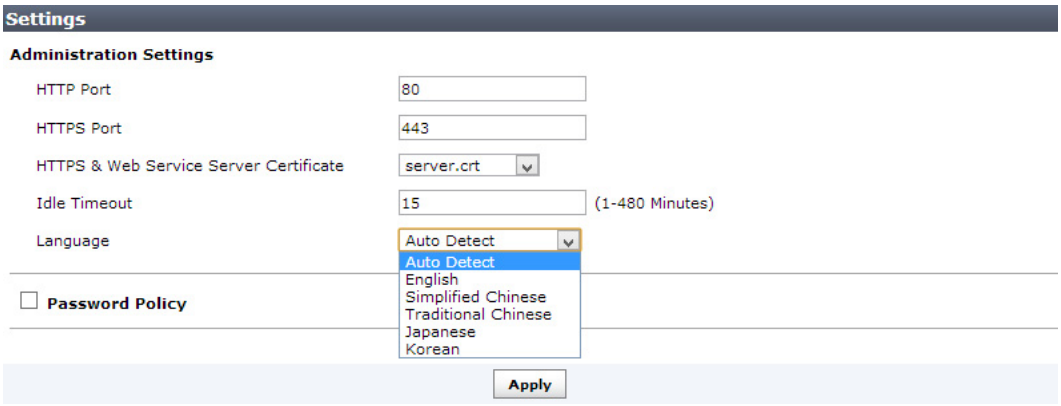
The Web-based Manager supports multiple languages; the default language setting is *Auto Detect*. *Auto Detect* uses the language configured on your management computer. If that language is not supported, the Web-based Manager will default to English.

You can change the Web-based Manager language to English, Simplified Chinese, Traditional Chinese, Japanese, or Korean. For best results, you should select the language that the management computer operating system uses.

To change the Web-based Manager language:

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

Figure 10: Administration 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 management computer.
3. Select *Apply*.

The following table lists FortiAnalyzer v5.0 Patch Release 6 language support information.

Table 2: Language support

Language	Web-based Manager	Reports	Documentation
English	✔	✔	✔
French	-	✔	-
Spanish	-	✔	-
Portuguese	-	✔	-
Korean	✔	✔	-
Chinese (Simplified)	✔	✔	-
Chinese (Traditional)	✔	✔	-
Japanese	✔	✔	-

Administrative access

Administrative access enables an administrator to connect to the system to view and change configuration settings. The default configuration of your system allows administrative access to one or more of the interfaces of the unit as described in the QuickStart and installation guides for your device.

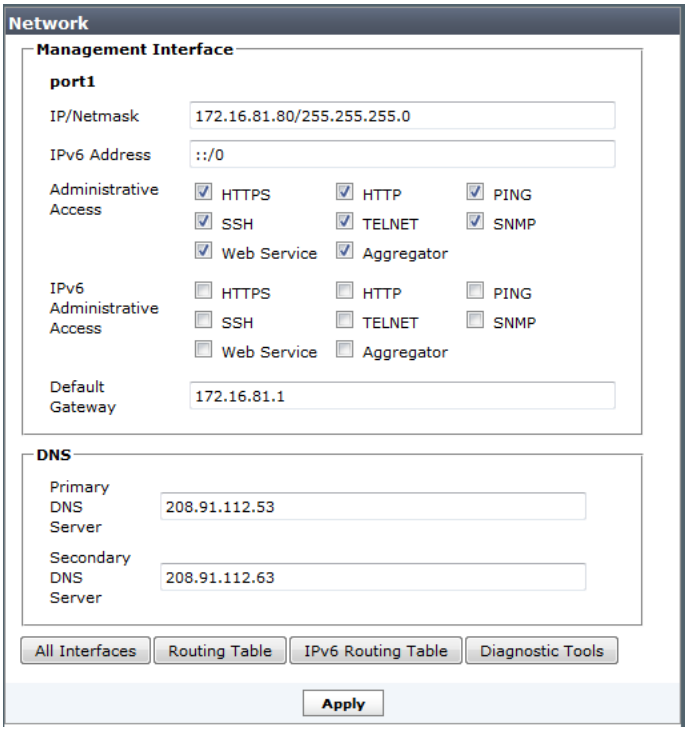
Administrative access can be configured in IPv4 or IPv6 and includes settings for: HTTPS, HTTP, PING, SSH, TELNET, SNMP, Web Service, and Aggregator.

To change administrative access:

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

   By default, port1 settings will be presented. To configure administrative access for a different interface, select *All Interfaces*, and then select the interface from the list.
2. Set the IPv4 *IP/Netmask* or the *IPv6 Address*, select one or more *Administrative Access* types for the interface, and set the default gateway and DNS servers.

Figure 11: Network management interface



3. Select *Apply* to finish changing the access settings.

   For more information, see "Network" on page 84.

Restricting access by trusted hosts

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 in to the Web-based Manager when working on a computer with the trusted host as defined in the admin account.

For more information, see "Administrator" on page 91.

Idle timeout

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

To change the Web-based Manager idle timeout:

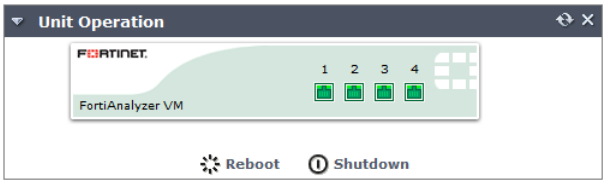
1. Go to *System Settings* > *Admin* > *Admin Settings* (see Figure 10 on page 34).
2. Change the *Idle Timeout* minutes as required.
3. Select *Apply* to save the setting.

   For more information, see "Administrator settings" on page 104.

Reboot and shutdown the FortiAnalyzer unit

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

Figure 12: Unit operation actions in the Web-based Manager



To reboot the FortiAnalyzer unit:

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

```
execute reboot
The system will be rebooted.
Do you want to continue? (y/n)
```

3. Select `y` to continue. The FortiAnalyzer system will be rebooted.

To shutdown the FortiAnalyzer unit:

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

```
execute shutdown
The system will be halted.
Do you want to continue? (y/n)
```

3. Select `y` to continue. The FortiAnalyzer system will be shut down.

To reset the FortiAnalyzer unit:

1. In the *CLI Console* widget, enter:

```
execute reset all-settings
This operation will reset all settings to factory defaults
Do you want to continue? (y/n)
```

2. Select `y` to continue. The device will reset to factory default settings and reboot.

To reset logs and re-transfer all logs into the database:

1. In the *CLI Console* widget, enter:

```
execute reset-sqllog-transfer
WARNING: This operation will re-transfer all logs into database.
Do you want to continue? (y/n)
```

2. Select `y` to continue.

Administrative Domains

When ADOMs are enabled, the *Device Manager* tab has collapsible ADOM navigation, where all of the ADOMs are displayed in the tree menu on the left of the interface. The devices within each ADOM are shown in the default *All FortiGate* group. When ADOMs are disabled, the tree menu simply displays *All FortiGates*, *All Log Arrays*, and *Unregistered Devices*, if there are any. Non-FortiGate devices are grouped into their own specific ADOMs.

ADOMs are not enabled by default, and enabling and configuring the domains can only be performed by the `admin` administrator. The maximum number of ADOMs you can add depends on the specific FortiAnalyzer system model. Please refer to the FortiAnalyzer datasheet for information on the maximum number of devices and ADOMs that your model supports.

The number of devices within each group is shown in parentheses next to the group name.

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. See "To enable the ADOM feature:" below.

You cannot create a new FortiMail or FortiWeb ADOM. Go to *System Settings* > *All ADOMs* to view all default and configured ADOMs on your FortiAnalyzer device. This page displays all the devices associated with each ADOM.

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*.
4. Select *OK* in the confirmation dialog box to enable ADOMs.

To disable the ADOM feature:

1. Remove all log devices from all non-root 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.
3. Go to *System Settings* > *Dashboard*.
4. In the system information widget, select *Disable* next to *Administrative Domain*.
5. Select *OK* in the confirmation dialog box to disable ADOMs.

Adding an ADOM

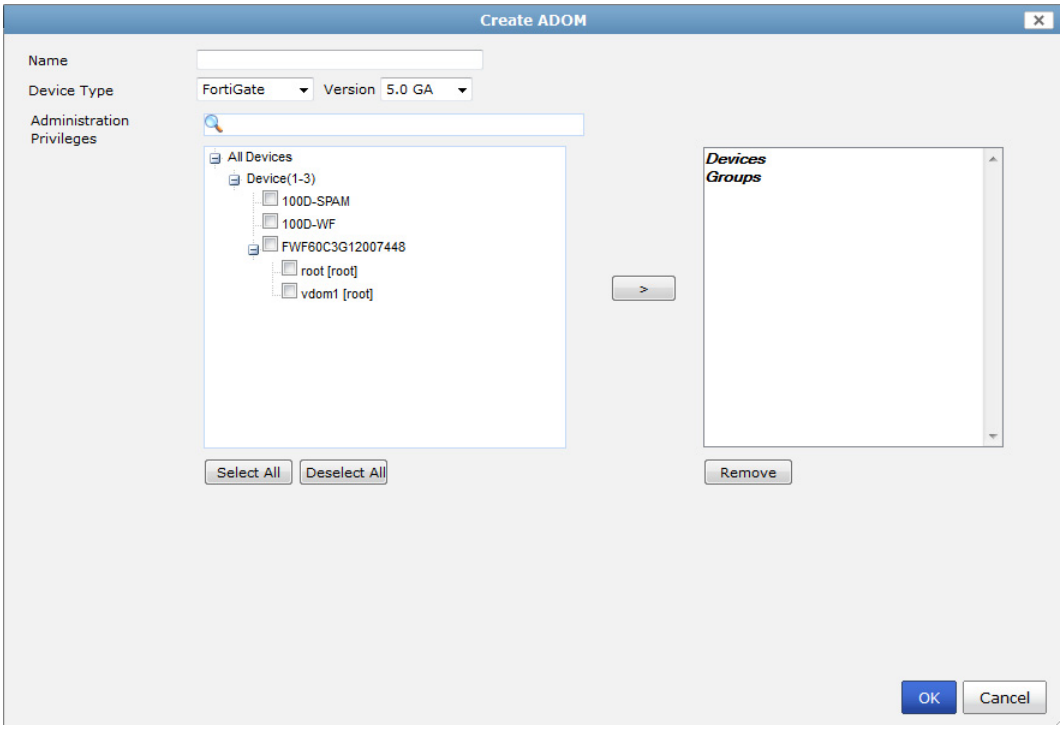
You can create both FortiGate and FortiCarrier ADOMs for versions 5.0, 4.0 MR3, and 4.0 MR2. FortiAnalyzer has default ADOMs for FortiCache, FortiCarrier, FortiClient, FortiMail, FortiWeb, FortiAnalyzer, and syslog devices. When one of these devices is promoted to the DVM table, the device is added to their respective default ADOM and will be visible in the tree menu.

To add an ADOM:

1. In the *Device Manager* tab, right-click on an ADOM name and, under the *ADOM* heading, select *Create New*. Alternatively, go to *System Settings* > *All ADOMs* and select *Create New* in the toolbar.

   The *Create ADOM* dialog box opens.

   Figure 13: Create an ADOM



2. Enter the following information:

Name	Enter an unique name that will allow you to distinguish this ADOM from your other ADOMs.
Device Type	Select the device type from the drop-down list. Select either FortiGate or FortiCarrier.
Version	Select the firmware version of the devices that will be in the ADOM. Select one the following: 5.0 GA, 4.0 MR3, or 4.0 MR2.
Search	Enter a search term to find a specific device (optional).
Devices	Transfer devices from the available member list on the left to the selected member list on the right to assign those devices to the ADOM.

3. Select *OK* to create the ADOM.

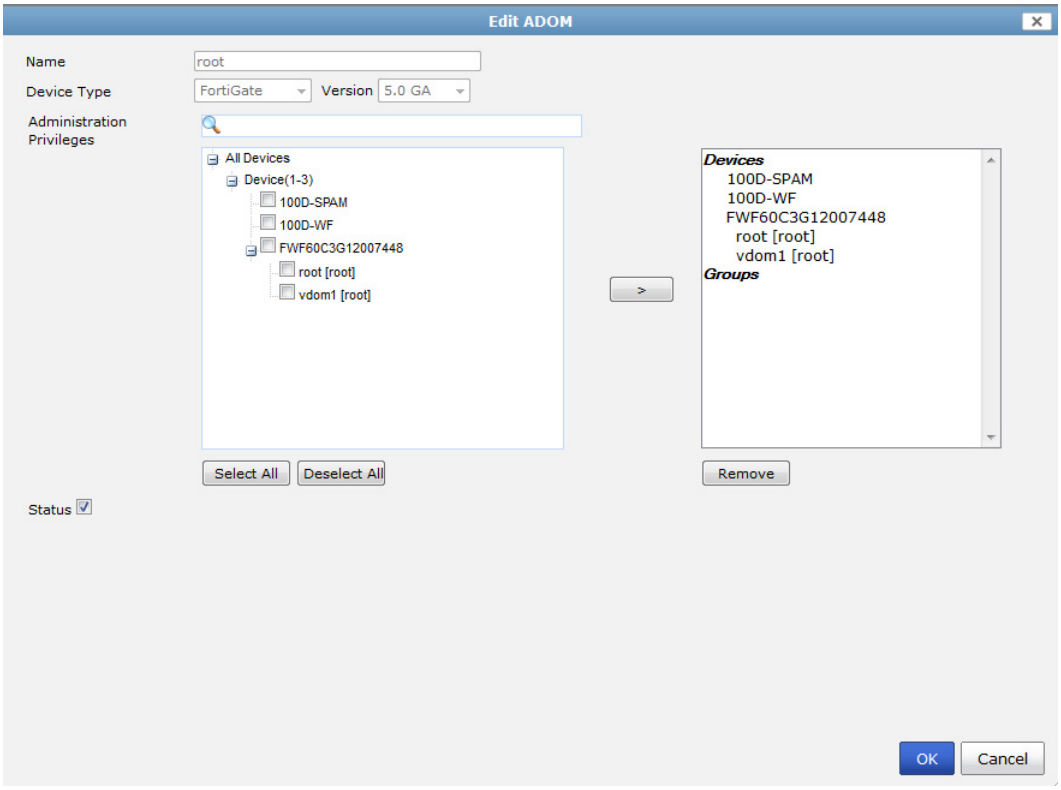
To edit an ADOM:

1. In the *Device Manager* tab, right-click on the ADOM you need to edit, then, under the *ADOM* heading, select *Edit*.

   Alternatively, go to *System Settings* > *All ADOMs*, right-click on the ADOM you need to edit, and select *Edit* in the right-click menu.

   The *Edit ADOM* dialog box opens.

   Figure 14: Edit an ADOM



2. Edit the following information as required:

Name	Edit the ADOM name.
Device Type	This field cannot be edited.
Version	This field cannot be edited.
Search	Enter a search term to find a specific device (optional).
Devices	Transfer devices from the available member list on the left to the selected member list on the right to assign those devices to the ADOM.
Status	Enable or disable the ADOM.

3. Select *OK* to finish editing the ADOM.

To delete an ADOM:

1. In the *Device Manager* tab, right-click on the ADOM you need to delete, and, under the *ADOM* heading, select *Delete*.

   Alternatively, go to *System Settings* > *All ADOMs*, right-click on the ADOM you need to delete, and select *Delete* in the right-click menu.

The root ADOM and ADOMs which contains user(s), device(s), or log array(s) cannot be deleted.

2. Select *OK* in the confirmation dialog box to delete the ADOM.

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*.

   Alternatively, go to *System Settings* > *All ADOMs*, right-click on the ADOM to which you want to assign a device and, and select *Edit* in the right-click menu

   The *Edit ADOM* dialog box will open.

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

   If the administrative device mode is *Advanced*, you can add separate FortiGate VDOMs to the ADOM as well as FortiGate units.

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

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

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 “Adding an ADOM” on page 39.

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.

4. Select *OK* to save the setting.

   See "Administrator" on page 91 for more information.

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.

Advanced ADOM mode will allow users to assign VDOMs from a single device to different ADOMs, but will result in a reduced operation mode and more complicated management scenarios. It is recommended for advanced users only.

To change the ADOM mode, go to *System Settings* > *Advanced* > *Advanced Settings* and change the selection in the *ADOM Mode* field.

Alternatively, use the following command in the CLI:

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

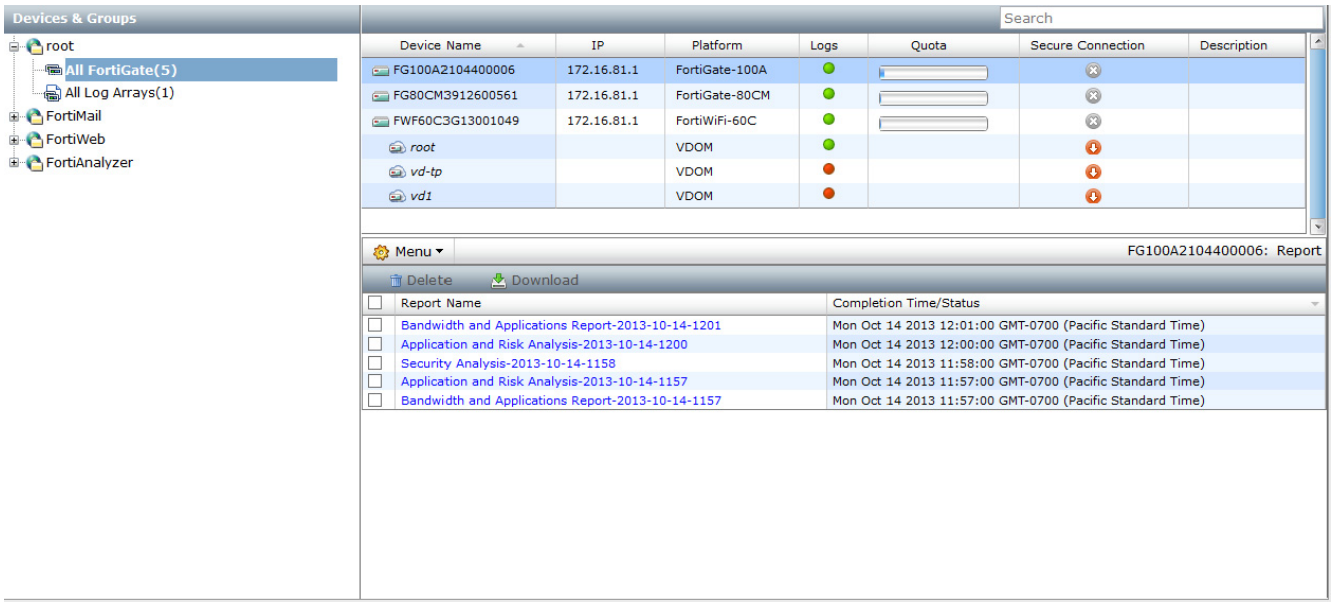
Normal mode is the default setting. To change from advanced back to normal, you must ensure no FortiGate VDOMs are assigned to an ADOM.

Device Manager

The *Device Manager* tab allows you to add and edit devices and VDOMs, and view real-time monitor data for those devices. It also allows you to create, edit, and delete ADOMs when they are enabled (see “System Information widget” on page 60). You can also configure log arrays for group-based access to logs and reports.

Figure 15 shows the Device Manager page.

Figure 15: Device Manager tab



The tree menu shows the ADOMs and the device and log arrays within those ADOMs. If ADOMs are disabled, the tree menu simply shows the devices and log arrays.

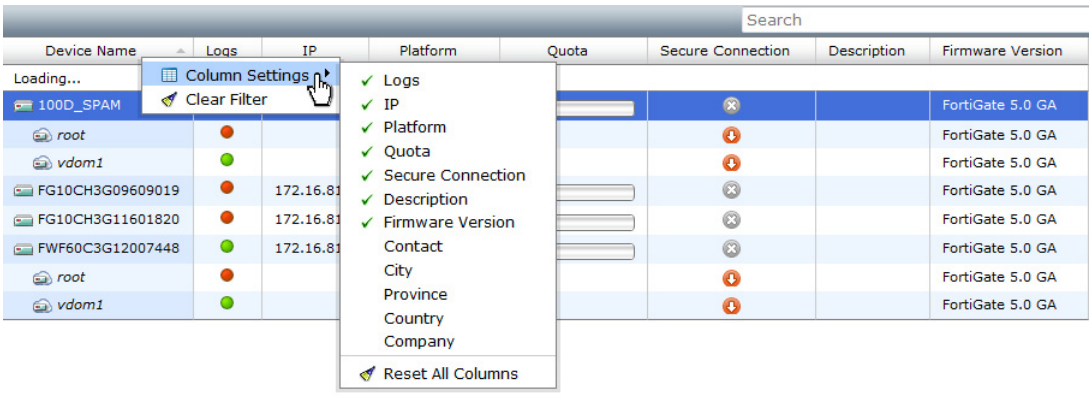
The device and VDOM list can be searched using the search box in the content pane toolbar. The columns shown in the list can be customized, and the list can be sorted by selecting a column header.

To change the column settings:

1. Right-click on a column heading in the content pane.
2. Select *Column Settings* in the right-click menu.

   Columns currently included in the content pane table have a green check mark next them.

   Figure 16: Column right-click menu



3. Select a column from the list to add or remove that column from the table.

   Select *Reset All Columns* to reset the table to its default state

Devices

Devices are organized by device type.

VDOMs and model devices can be created and deleted, and added to log arrays to help organize the devices and VDOMs and to simplify the process of updating their firmware. See “Log arrays” on page 51 for more information.

Devices and VDOMs

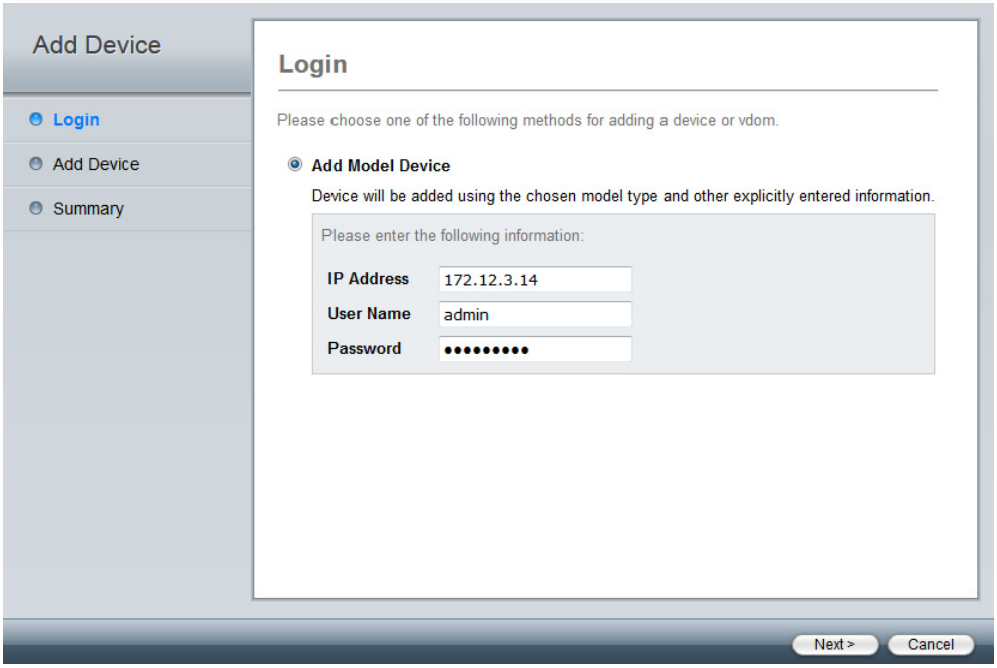
Device models can be added and deleted, devices can be edited, and VDOMs can be deleted. The *Add Device* wizard is used to add model devices.

To add a model device:

1. Right-click on a group in the tree menu or in the content pane and, from the right-click menu, select *Add Device*, or, if ADOMs are not enabled, select *Add Device* from the toolbar.

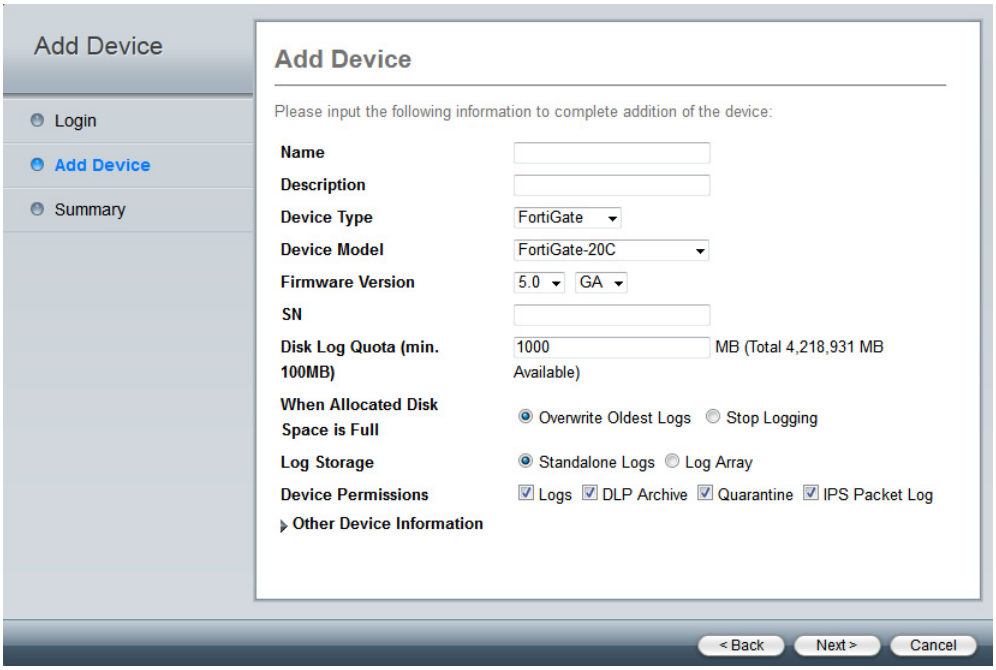
   The *Add Device* wizard opens.

   Figure 17: Add device wizard login screen



2. Enter the device IP address, name, and password in the requisite fields.
3. Select *Next* to continue to the next page of the wizard: *Add Device*.

Figure 18: Add device wizard add device screen



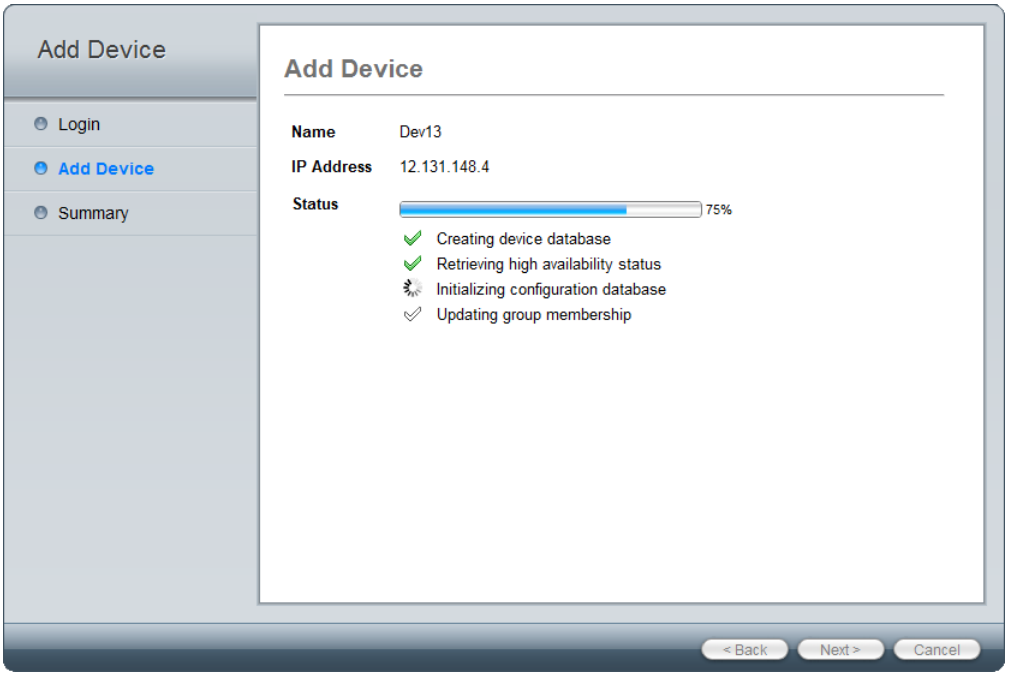
4. Enter the following information:

Name	Enter a name for the device.
Description	Enter a description for the device (optional).
Device Type	Select the device type from the drop-down list. Select FortiGate for FortiGate ADOMs, FortiSwitch for FortiSwitch ADOMs, etc.
Device Model	Select the device model from the drop-down list.
Firmware Version	Select the firmware version and major release from 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 (min. 100MB)	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.
Log Storage	Select either Standalone Logs or Log Array. When selecting Log Array, select the array from the drop-down list.
Device Permissions	Select the device permissions from: *Logs, DLP Archive, Quarantine*, and *IPS Packet Log*.

Central FortiAP	Select to enable or disable central FortiAP. This option is only available for certain device types.
Add to Groups	Select *Specify*, and then specify the groups this device model will be added to, or select *None*. This option is only available for certain device types.
Other Device Information	Enter other device information (optional), including: Company/Organization, Contact, City, Province/State, and Country.

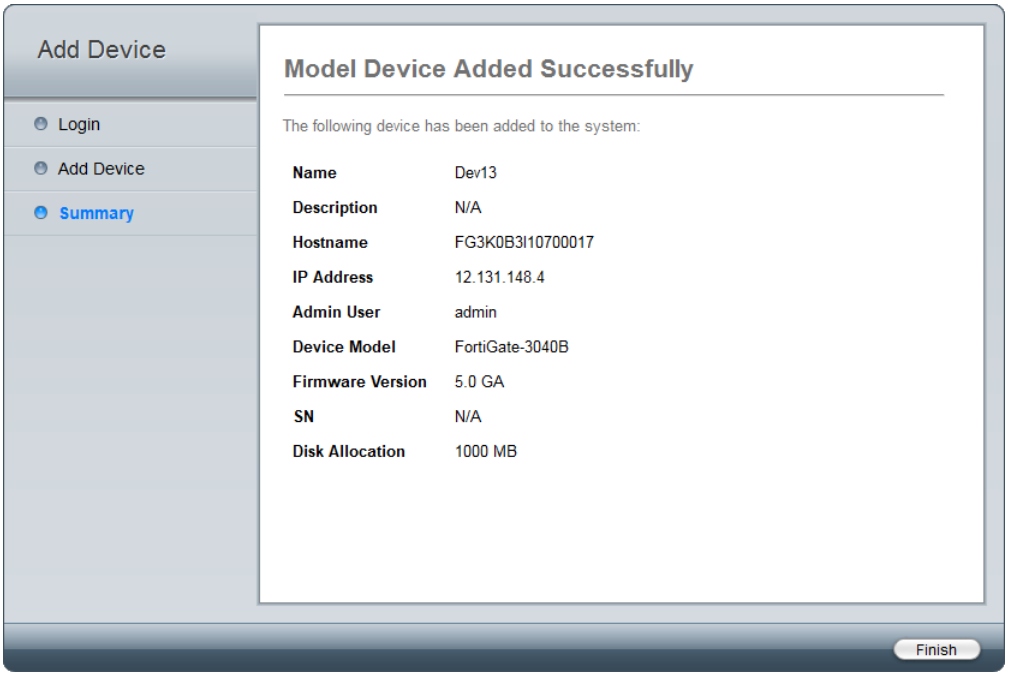
5. Select *Next* to proceed to the next add device page.

Figure 19: Add device wizard add device screen two



6. After the device has been created successfully, select *Next* to proceed to the summary page.

Figure 20: Add device wizard summary screen



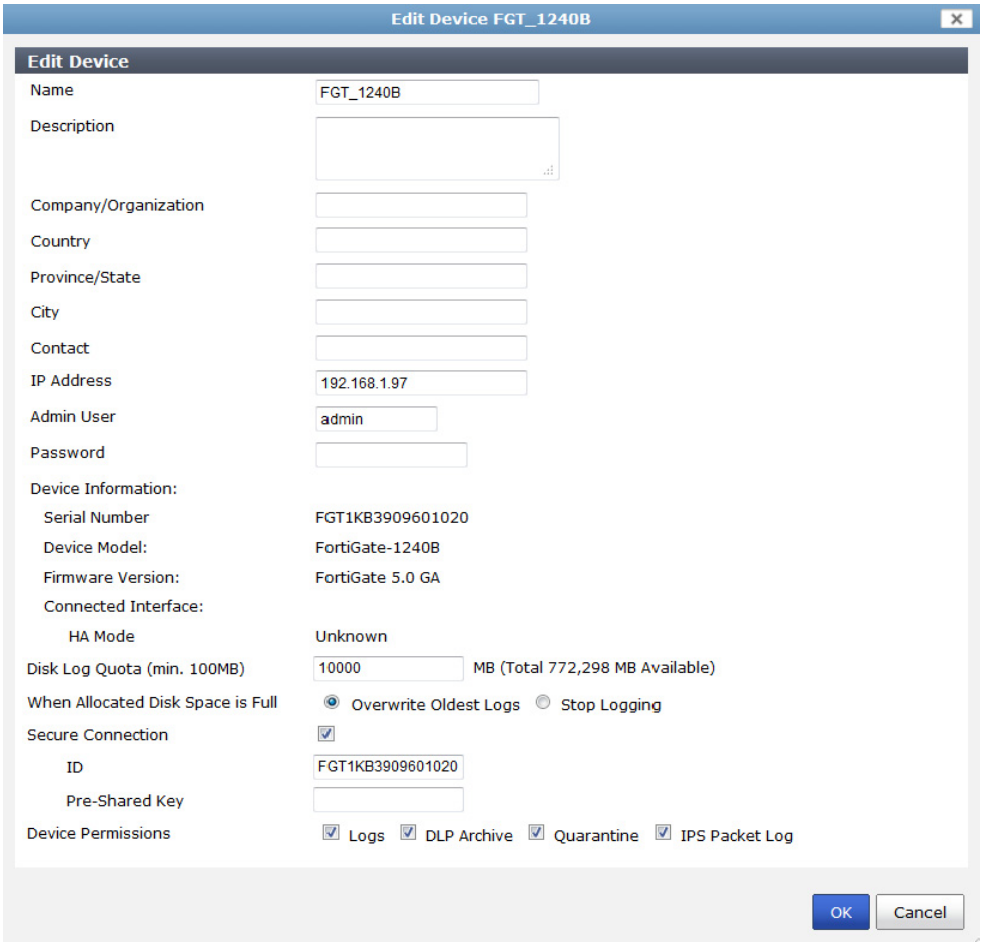
7. Select *Finish* to add the device model.

To edit a device:

1. In the *Device Manager* tab, in the tree menu, select the group that contains the device you need to edit.
2. In the content pane, right-click on the on the device and select *Edit* from the right-click menu.

   The *Edit Device* dialog box opens.

Figure 21: Edit a device



3. Edit the following information as needed:

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 administrator username.
Password	The administrator 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 (min. 100MB)	The amount of space that the disk log is allowed to use, in MB.
When Allocated Disk Space is Full	The action for the system to take when the disk log quota is filled, either *Overwrite Oldest Logs*, or *Stop Logging*.
Secure Connection	Select check box to enable this feature. Secure Connection secures OFTP traffic through an IPsec tunnel.
ID	The device serial number.
Pre-Shared Key	The pre-shared key for the IPsec connection between the FortiGate and FortiAnalyzer.
Device Permissions	The device's permissions. Select any of: *Logs*, *DLP Archive*, *Quarantine*, and *IPS Packet Log*.

4. Select *OK* to finish editing the device.

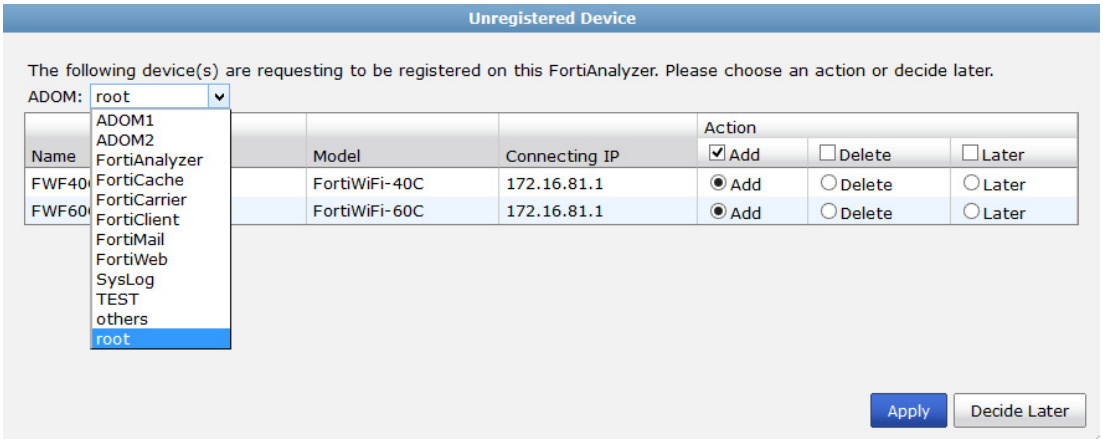
To delete a device or VDOM:

1. In the *Device Manager* tab, in the tree menu, select the group that contains the device or VDOM you need to delete.
2. In the content pane, right-click on the on the device or VDOM and select *Delete* in the right-click menu.
3. Select *OK* in the confirmation window to delete the device or VDOM.

Unregistered devices

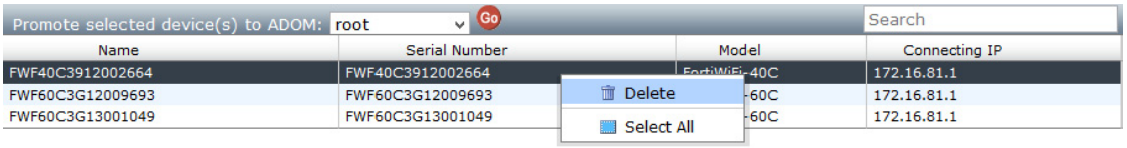
In FortiAnalyzer v5.0 Patch Release 4 or earlier releases, the `config system global set unregister-pop-up` command is enabled by default. When a device is configured to send logs to FortiAnalyzer, the unregistered device table will be displayed. You can decide to add devices to specific ADOMs now, at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

Figure 22: Unregistered device dialog box



In FortiAnalyzer 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 FortiAnalyzer, the unregistered device table will not be displayed. Instead, a new entry *Unregistered Devices* will appear in the Device Manager tab tree menu. You can then promote devices to specific ADOMs or use the right-click menu to delete the device.

Figure 23: Promote unregistered devices



Log arrays

Log arrays support group-based access to logs and reports. They also allow you to manage log data belonging to FortiGate HA clusters from a single device object. You can add VDOMs from a single device to different log arrays, and configure and schedule reports for each log array.

Both the device disk log quota and the log array disk log quota are enforced. The device disk log quota includes all log files, all archive files, and database space for logs on the device. The log array disk log quota includes database space used by log array tables. The device disk log quota no longer applies when it is added to a 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 FortiAnalyzer device.

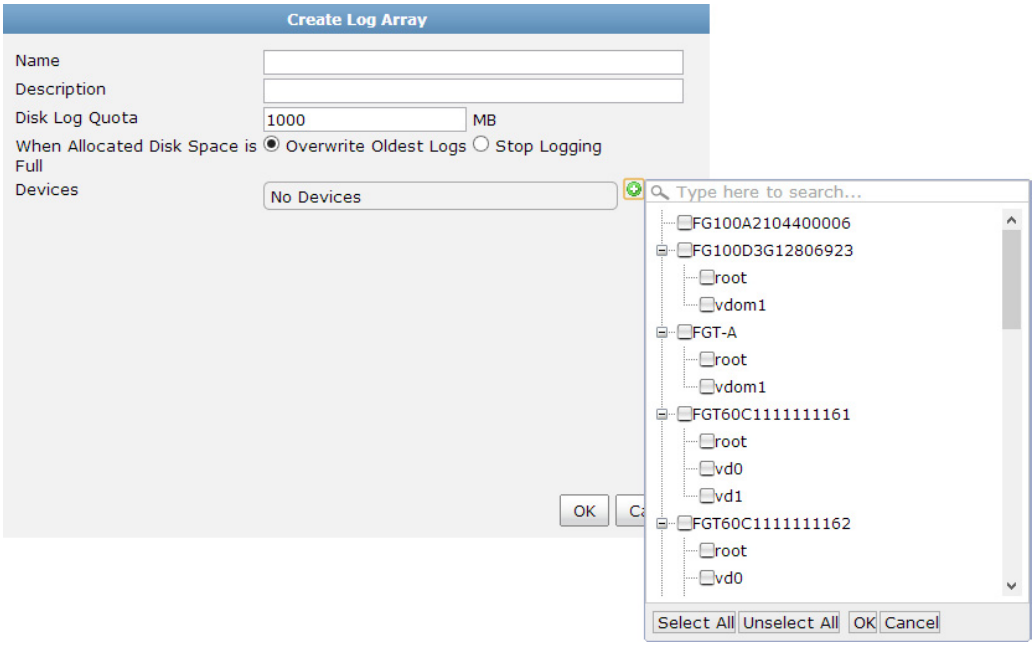
Fortinet recommends configuring log arrays prior to deploying the FortiAnalyzer into production. When adding and deleting log arrays, you will need to rebuild the database to view older logs.

To create a new log array:

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

   The *Create Log Array* window opens.

Figure 24: Create log array window



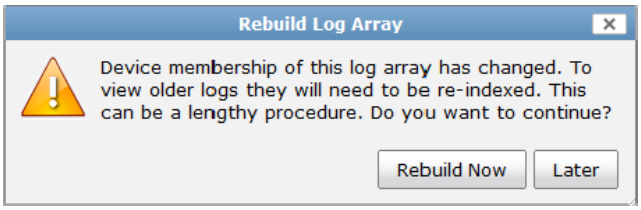
2. Configure the following settings:

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. You can add VDOMs from a single device to different log arrays. Select *OK* in the pop-up dialog box once you have selected all of the devices an VDOMs that you would like to add to the log array.

3. Select *OK* to save the log array configuration.
4. You will be prompted to rebuild the log array.

Figure 25: Rebuild log array dialog box



5. Select to rebuild the log array now or at a later date. To view older logs they will need to be re-indexed.

To edit a log array:

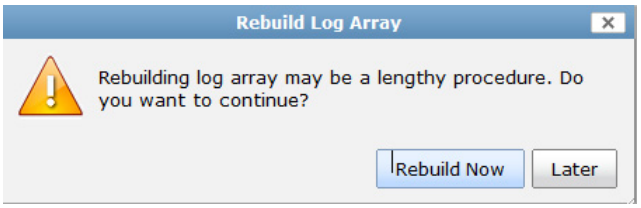
1. In the *Device Manager* tab, select *All Log Arrays* from the navigation tree.
2. In the right content pane, right-click the log array you would like to edit and select *Edit* in the right-click menu.
3. Edit the settings as required.
4. Select *OK* to save the changes.

To rebuild a log array:

1. In the *Device Manager* tab, select *All Log Arrays* from the navigation tree.
2. In the right content pane, right-click the log array you would like to rebuild and select *Rebuild* in the right-click menu.

   The *Rebuild Log Array* dialog box opens.

Figure 26: Rebuild log array dialog box.



3. Select *Rebuild Now* to continue.

To delete a log array:

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

Device reports

You can view, download, and delete device reports in the Device Manager content pane. Selecting a device or VDOM from the list will display all reports associated with that device or VDOM. For more information, see "Completed reports" on page 165.

To view latest reports from the Device Manager tab:

1. In the *Device Manager* tab select the ADOM that contains the device or log array whose reports 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.
3. You can click on the report to display the report in a browser window or download the report to your management computer.

Log forwarding

When your FortiAnalyzer device is configured in collector mode, you can configure log forwarding in the Device Manager tab. You can configure to forward logs for selected devices to another FortiAnalyzer, a syslog server, or a Common Event Format (CEF) server.

To put your FortiAnalyzer in collector mode:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Operation Mode* field, select *[Change]*.
3. In the *Change Operation Mode* dialog box, select *Collector*, and then select *OK*.

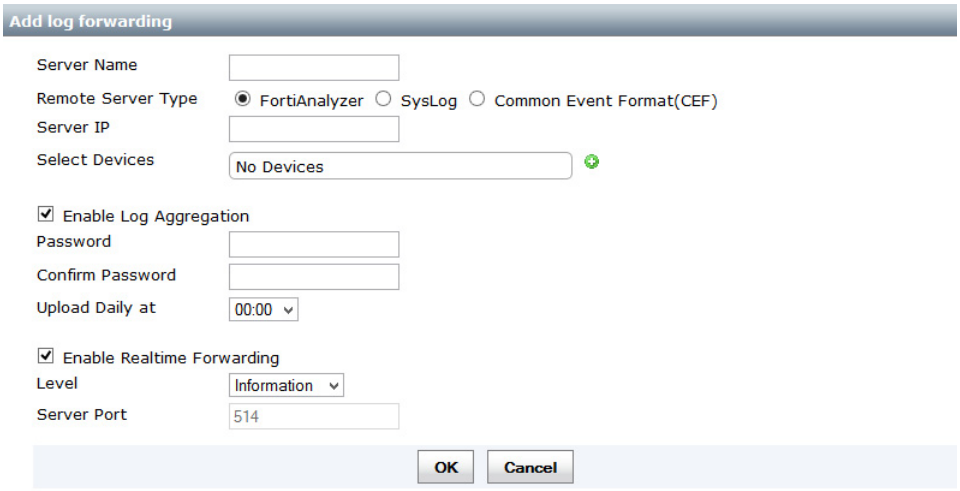
   The Web-based Manager will refresh and the Device Manager, Log View, and System Settings tabs are available. See "Changing the operation mode" on page 65 for more information.

To configure log forwarding:

1. Go to the *Device Manager* tab and select *Log Forwarding*.
2. Select *Create New* from the toolbar.

   The *Add log forwarding* page is displayed.

Figure 27: Add log forwarding dialog box



3. Configure the following settings:

Server Name	Enter a name to identify the remote server.
Remote Server Type	Select the remote server type. Select one of the following: *FortiAnalyzer*, *Syslog*, *Common Event Format (CEF)*.
Server IP	Enter the server IP address.
Select Devices	Select the add icon to select devices. Select devices and select *OK* to add the devices.
Enable Log Aggregation	Select to enable log aggregation. This option is available when *Remote Server Type* is *FortiAnalyzer*.
Password	Enter the server password.
Confirm Password	Re-enter the server password.
Upload Daily at	Select a time from the drop-down list.
Enable Realtime Forwarding	Select to enable realtime log forwarding.
Level	Select the logging level from the drop-down list. Select one of the following: *Emergency, Alert, Critical, Error, Warning, Notification, Information*, or *Debug*.
Server Port	Enter the server port. When *Remote Server Type* is *FortiAnalyzer*, the port cannot be changed. The default port is 514.

4. Select *OK* to save the setting.

System Settings

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

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

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

Dashboard	Select this menu to configure, monitor, and troubleshoot your FortiAnalyzer device. Dashboard widgets include: System Information, License Information, Unit Operation, System Resources, Alert Message Console, CLI Console, Log Receive Monitor, Logs/Data Received, and Statistics.
All ADOMs	Select this menu to create new ADOMs and monitor all existing ADOMs.
RAID Management	Select this menu to configure and monitor your Redundant Array of Independent Disks (RAID) setup. This page displays information about the status of RAID disks as well as what RAID level has been selected. It also displays how much disk space is currently consumed.
Network	Select this menu to configure your FortiAnalyzer interfaces. You can also view the IPv4/IPv6 Routing Table and access Diagnostic Tools.
Admin	Select this menu to configure administrator user accounts, as well as configure global administrative settings for the FortiAnalyzer unit. • Administrator • Profile • Remote authentication server • Administrator settings
Certificates	Select this menu to configure the following: • Local certificates • CA certificates • Certificate revocation lists
Event log	Select this menu to view FortiAnalyzer event log messages. On this page you can: • Download the logs in .log or .csv formats • View raw logs or logs in a formatted table • Browse the event log, FDS upload log, and FDS download log

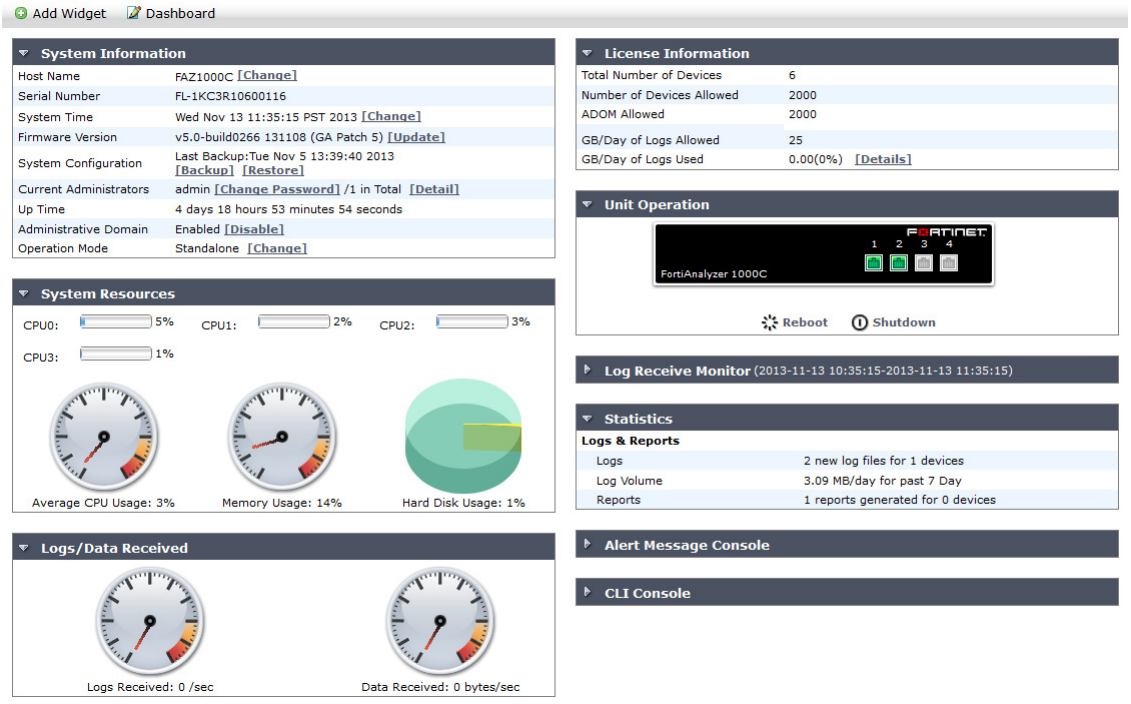
Task monitor	Select this menu to monitor FortiAnalyzer tasks.
Advanced	Select to configure advanced settings. • SNMP v1/v2c • Mail server • Syslog server • Meta fields • Device log settings • File management • Advanced settings

Dashboard

When you select the *System Settings* tab, it automatically opens at the *System Settings* > *Dashboard* page; see Figure 28.

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

Figure 28: FortiAnalyzer system settings dashboard



The following widgets are available:

System Information	Displays and allow editing of some basic information about the FortiAnalyzer system, including host name, serial number, platform type, system time, firmware version, system configuration, current administrators, up time, administrative domains, and operation mode. From this widget you can manually update the FortiAnalyzer firmware to a different release. For more information, see "System Information widget" on page 60.
License Information	Displays the devices being managed by the FortiAnalyzer unit, the maximum numbers of devices allowed, the maximum number of ADOMs allowed, GB/Day of logs allowed, and GB/Day of logs used. FortiAnalyzer VM also includes device quota allowed, device quota used, and management IP address fields. For more information, see "License Information widget" on page 66.
Unit Operation	Displays status and connection information for the ports of the FortiAnalyzer unit. It also enables you to shutdown and reboot the FortiAnalyzer unit. For more information, see "Unit Operation widget" on page 67.
System Resources	Displays the real-time and historical usage status of the CPU, memory and hard disk. For more information, see "System Resources widget" on page 68.
Alert Message Console	Displays log-based alert messages for both the FortiAnalyzer unit itself and connected devices. For more information, see "Alert Messages Console widget" on page 70.
CLI Console	Opens a terminal window that enables you to configure the FortiAnalyzer unit using CLI commands directly from the Web-based Manager. For more information, see "CLI Console widget" on page 71.
Statistics	Displays statistics for logs and reports since last reset. For more information, see "Statistics widget" on page 72.
Logs/Data Received	Displays the real-time or historical usage status of logs received and data received. For more information, see "Logs/Data Received widget" on page 72.
Log Receive Monitor	Displays a real-time graph 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 73.

Customizing the dashboard

The FortiAnalyzer system settings dashboard is customizable. You can select which widgets to display, where they are located on the page, and whether they are minimized or maximized.

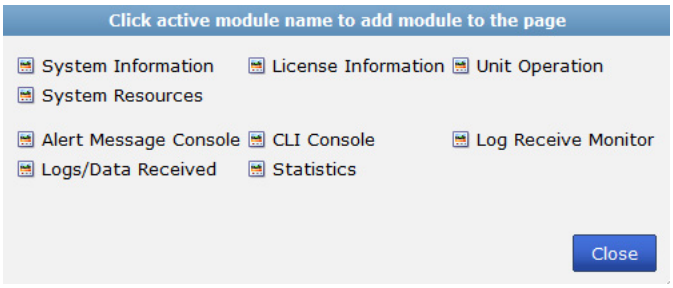
To move a widget

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 29: Click an active module name to add module to page dialog box



To reset the dashboard

In the dashboard toolbar, select *Dashboard* > *Reset Dashboards*. The dashboards will be reset to the default view, which includes everything except the *CLI Console* widget.

To see the available options for a widget

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

Figure 30:A minimized widget

The following table lists the widget options.

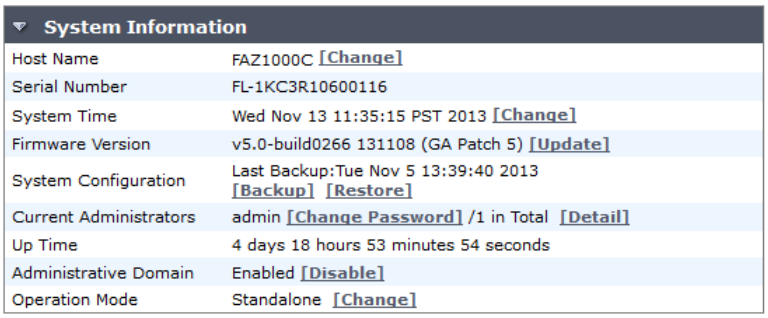
Show/Hide arrow	Display or minimize the widget.
Widget Title	The name of the widget.
More Alerts	Show the *Alert Messages* dialog box. This option appears only in the *Alert Message Console* widget.
Edit	Select to change settings for the widget. This option appears only in certain widgets.

Detach	Detach the *CLI Console* widget from the dashboard and open it in a separate window. This option appears only in the *CLI Console* widget.
Reset	Select to reset the information shown in the widget. This option appears only in the *Statistics* widget.
Refresh	Select to update the displayed information.
Close	Select to remove the widget from the dashboard. You will be prompted to confirm the action.

System Information widget

The *System Information* widget, shown in Figure 31, displays the current status of the FortiAnalyzer unit and enables you to configure basic system settings.

Figure 31: System information widget



The following information is available on this widget:

Host Name	The identifying name assigned to this FortiAnalyzer unit. For more information, see "Changing the host name" on page 61.
Serial Number	The serial number of the FortiAnalyzer unit. The serial number is unique to the FortiAnalyzer unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
Platform Type	This field is displayed for FortiAnalyzer VM and shows the VM platform type on which the FortiAnalyzer is installed.
System Time	The current date, time, and time zone on the FortiAnalyzer internal clock or NTP server. For more information, see "Setting the date and time" on page 62.
Firmware Version	The version number and build number of the firmware installed on the FortiAnalyzer unit. To update the firmware, you must download the latest version from the Customer Service & Support portal at https://support.fortinet.com. Select *Update* and select the firmware image to load from your management computer. For more information, see "Updating the system firmware" on page 63.

System Configuration	The date of the last system configuration backup. The following actions are available: • Select *Backup* to backup the system configuration to a file; see "Backing up the system" on page 64. • Select *Restore* to restore the configuration from a backup file; see "Restoring the configuration" on page 65.
Current Administrators	The number of administrators that are currently logged in. The following actions are available: • Select *Change Password* to change your own password. • Select *Details* to view the session details for all currently logged in administrators. See "Monitoring administrator sessions" on page 90 for more information.
Up Time	The duration of time the FortiAnalyzer unit has been running since it was last started or restarted.
Administrative Domain	Displays whether ADOMs are enabled, and allows for enabling and disabling ADOMs. See "Administrative Domains" on page 38 for more information.
Operation Mode	Display and change the current operating mode. Note that not all models support all operation modes. See "Changing the operation mode" on page 65.

Changing the host name

The host name of the FortiAnalyzer 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 60.
- 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 113.

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.

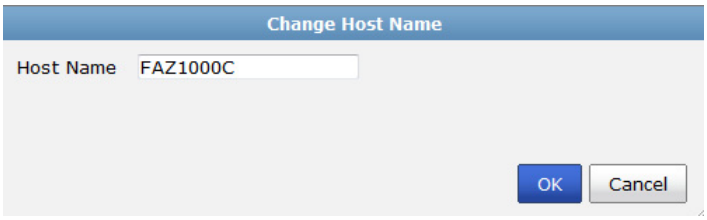
For example, if the host name is Fortinet1234567890, the CLI prompt would be `Fortinet123456~#`.

To change the host name:

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

   The *Change Host Name* dialog box appears.

   Figure 32: Change 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* to save the setting.

Setting the date and time

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

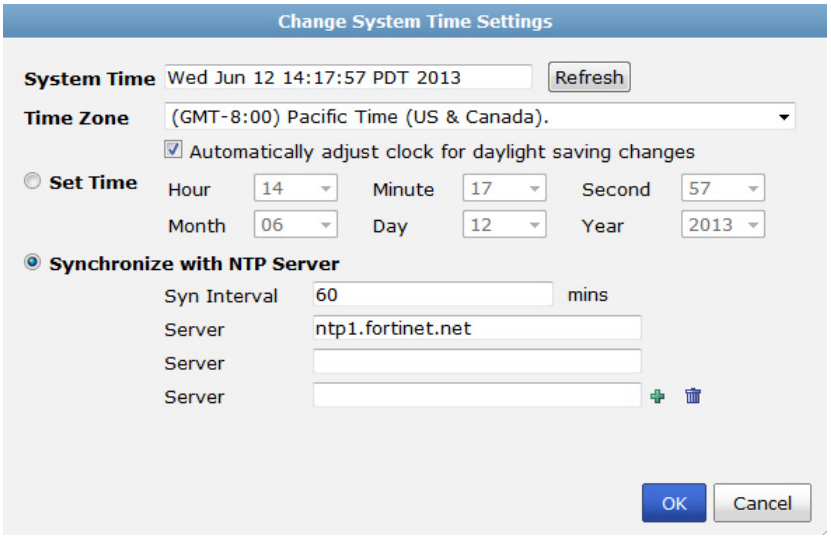
For many features to work, including scheduling, logging, and SSL-dependent features, the FortiAnalyzer system time must be accurate.

To configure the date and time:

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

   The *Change System Time Settings* dialog box appears.

Figure 33: Change system time settings dialog box



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

System Time	The date and time according to the FortiAnalyzer unit's clock at the time that this tab was loaded, or when you last selected the *Refresh* button for the *System Information* widget.
Time Zone	Select the time zone in which the FortiAnalyzer 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 FortiAnalyzer 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 FortiAnalyzer unit's clock with an NTP server, then configure the *Syn Interval* and *Server* fields before you select *OK*. Select the plus (+) icon to add multiple NTP servers.
Sync Interval	Enter how often in minutes the FortiAnalyzer 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, the device firmware can be upgraded. For more information on firmware upgrades see "FortiAnalyzer Firmware" on page 195.

For information about a specific firmware version, see the *FortiAnalyzer Release Notes* in the Fortinet Document Library.

Backing up the system

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

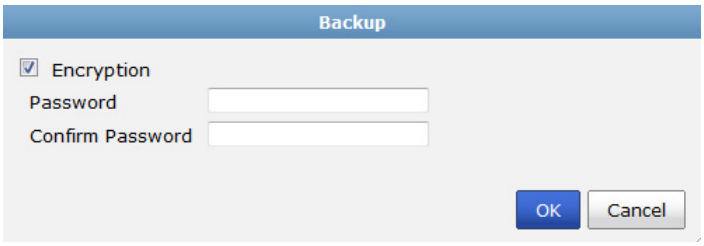
You can perform backups manually. Fortinet recommends backing up all configuration settings from your FortiAnalyzer unit before upgrading the FortiAnalyzer firmware.

To back up the FortiAnalyzer configuration:

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

   The *Backup* dialog box appears.

Figure 34: 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	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 FortiAnalyzer configuration from a backup file on your management computer.

To restore the FortiAnalyzer configuration:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *System Configuration* field, select *Restore*.

   The *Restore* dialog box appears.

Figure 35: Restore dialog box

3. Configure the following settings:

From Local	Select *Browse* to find the configuration backup file you want to restore on your management computer.
Password	Enter the encryption password, if applicable.
Overwrite current IP, routing	Select the check box if you need to overwrite the current IP and routing settings.

4. Select *OK* to proceed with the configuration restore.

Changing the operation mode

The FortiAnalyzer unit has two operation modes: analyzer and collector. For more information, see “Operation modes” on page 26.

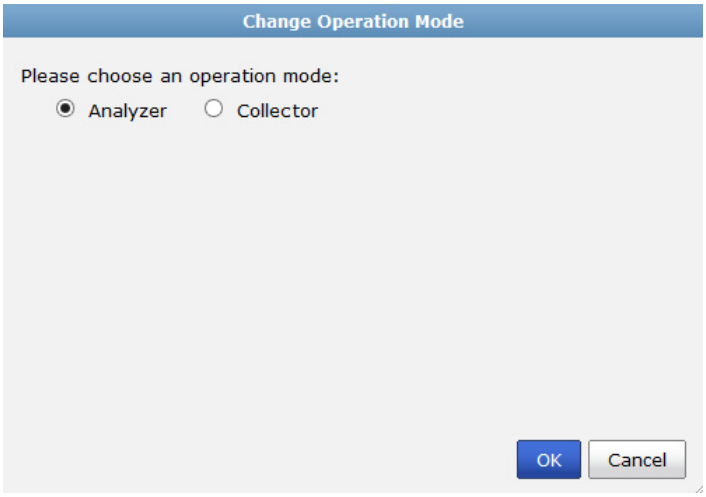
Not all FortiAnalyzer models support all operation modes.

To change the operation mode:

1. On the FortiAnalyzer unit, go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Operation Mode* field, select *Change*.

   The *Change Operation Mode* dialog box opens.

Figure 36: Change operation mode



3. Configure the following settings:

Analyzer	Select to configure FortiAnalyzer in analyzer mode.
Collector	Select to configure FortiAnalyzer in collector mode.

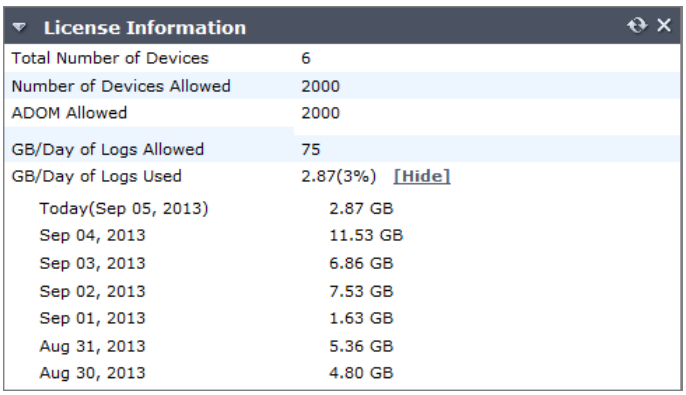
4. Select *OK* to change the operation mode.

License Information widget

The license information displayed on the dashboard shows information on features that vary by a purchased license or contract, such as FortiGuard subscription services. It also displays how many devices are connected or attempting to connect to the FortiAnalyzer unit.

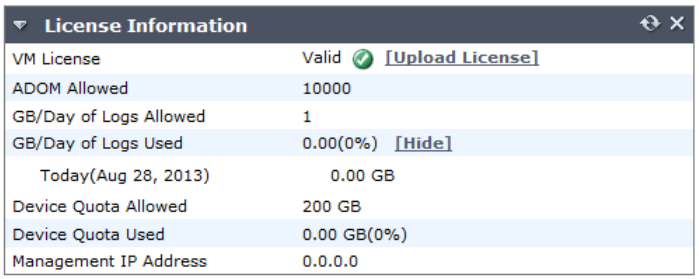
The information displayed in the license information widget will vary between physical and virtual machine FortiAnalyzer variations.

Figure 37: License information widget



The VM license information widget displays similar information but includes the VM license information and management IP address.

Figure 38:VM License information widget



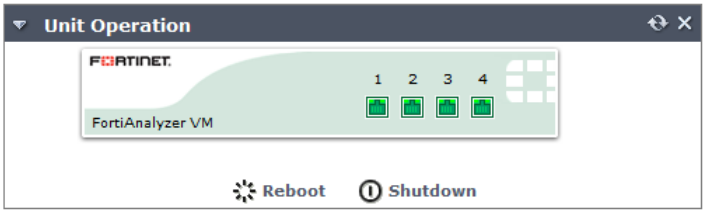
Upload a FortiAnalyzer VM license:

1. Go to *System Settings* > *Dashboard*.
2. In the *License Information* widget, in the *VM License* field, select *Upload License*.
3. Browse to the VM license file on your management computer.
4. Select *OK* to load the license file.

Unit Operation widget

The *Unit Operation* widget on the dashboard is a graphical representation of the FortiAnalyzer unit. It displays status and connection information for the ports on the FortiAnalyzer unit. It also enables you to quickly reboot or shutdown the FortiAnalyzer device.

Figure 39: Unit operation widget



The following information is available on this widget:

Port numbers (vary depending on model)	The image below the port name indicates its status by its color. Green indicates the port is connected. Grey indicates there is no connection. For more information about a port's configuration and throughput, position your mouse over the icon for that port. A pop-up box displays 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 FortiAnalyzer unit. You are prompted to confirm before the reboot is executed.
Shutdown	Select to shutdown the FortiAnalyzer unit. You are prompted to confirm before the shutdown is executed.

System Resources widget

The *System Resources* widget on the dashboard displays the usage status of the CPU, memory and hard disk. You can view system resource information in real-time or historical format, and either the average CPU usage or the usage for each individual processor core.

Figure 40: System resources widget (real time display)

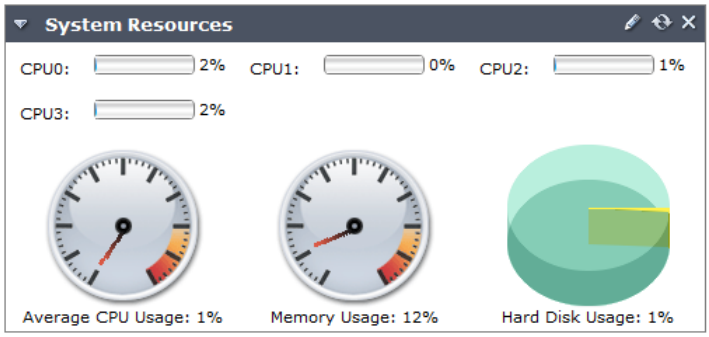
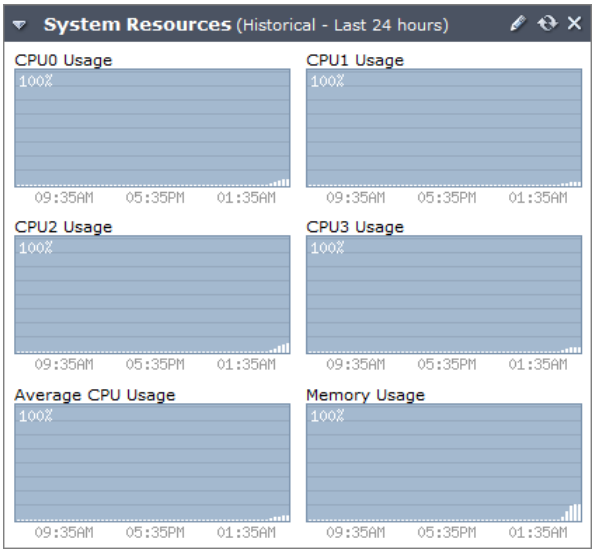


Figure 41: System resources widget (historical display)



The following information is available:

CPUx Usage	The current CPU utilization for each processor core. 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.
Average CPU Usage	The current average CPU utilization. The Web-based Manager displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the Web-based Manager) is excluded.

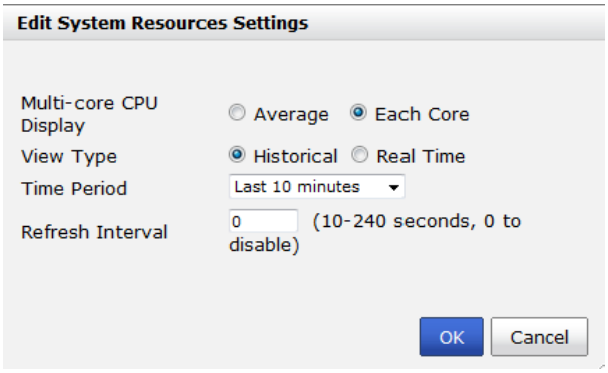
Memory Usage	The current memory utilization. The Web-based Manager displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.
Hard Disk Usage	The current hard disk usage, shown on a pie chart as a percentage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

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 42: Edit system resources settings window



3. You can configure the following settings:

Multi-core CPU Display	Select *Each Core* to view the CPU usage for each processor core (default). Select *Average* to view only the average CPU usage.
View Type	Select *Real Time* to view the most current information about system resources (default). Select *Historical* to view historical information about system resources.
Time Period	Select one of the following: *Last 10 minutes*, *Last 1 hour,* or *Last 24 hours*. This option is only available when *Historical* is selected.
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*.

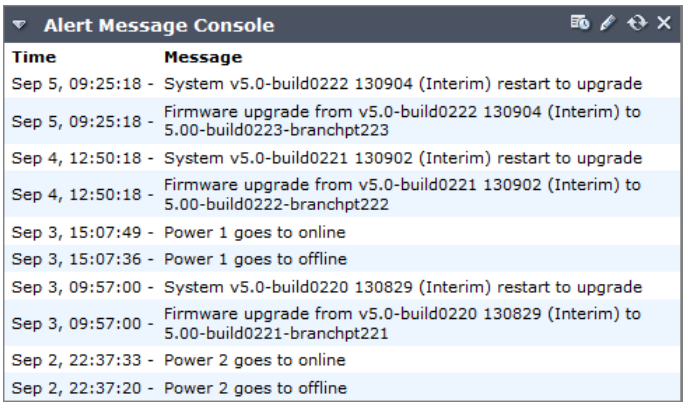
4. Select *OK* to apply your settings.

Alert Messages Console widget

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

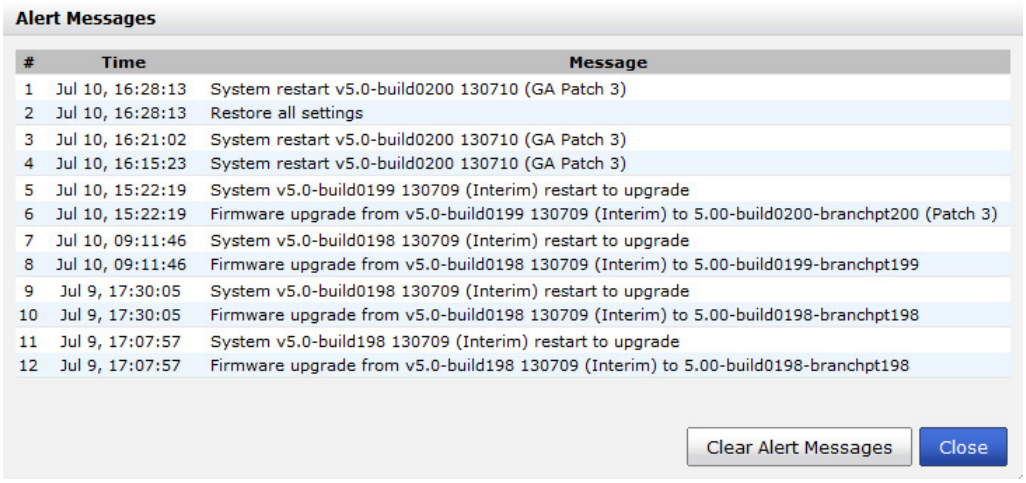
Alert messages help you track system events on your FortiAnalyzer unit such as firmware changes, and network events such as detected attacks. Each message shows the date and time that the event occurred.

Figure 43: Alert message console widget



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

Figure 44: 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 that are visible, and their refresh interval.

CLI Console widget

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

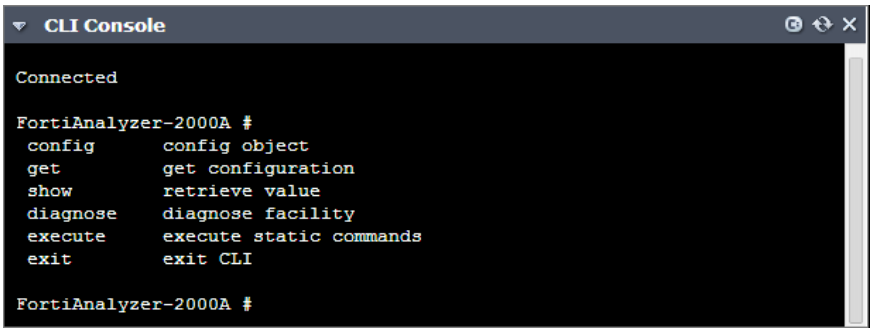
The *CLI Console* widget requires that your web browser support JavaScript.

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

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

For information on available CLI commands, see the *FortiAnalyzer v5.0 CLI Reference*.

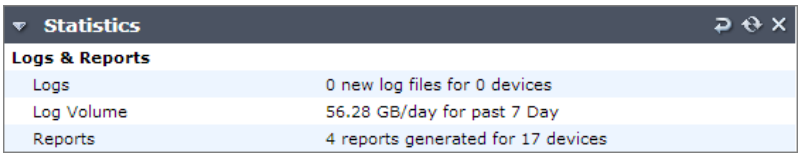
Figure 45:CLI console widget



Statistics widget

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

Figure 46: Statistics widget



The widget displays the following information:

Logs & Reports	
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.
Reset	Select *Reset* to reset the aforementioned statistics back to zero.

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 FortiAnalyzer unit.

Figure 47: Logs/data received widget (real-time)

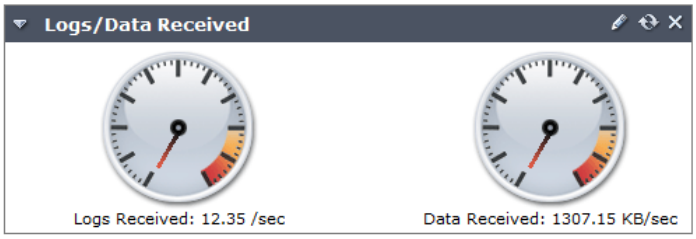
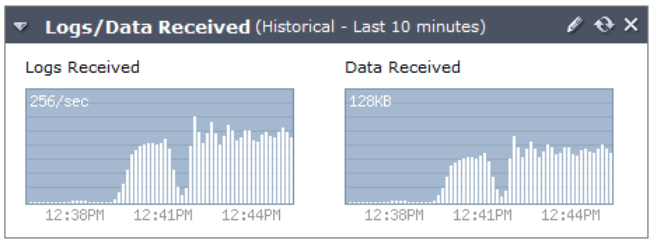


Figure 48: Logs/data received widget (historical)

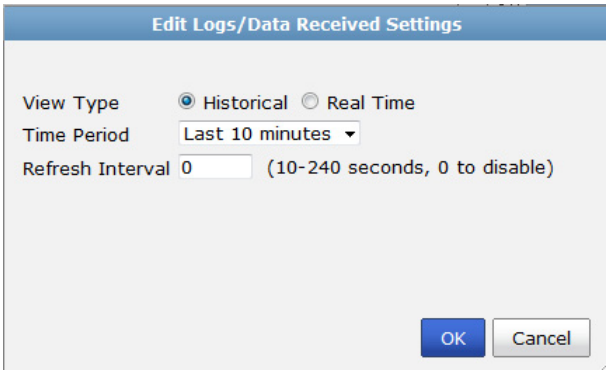


The widget displays the following information:

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

To configure settings for the widget, select *Edit* from the title bar.

Figure 49: Edit logs/data received settings window



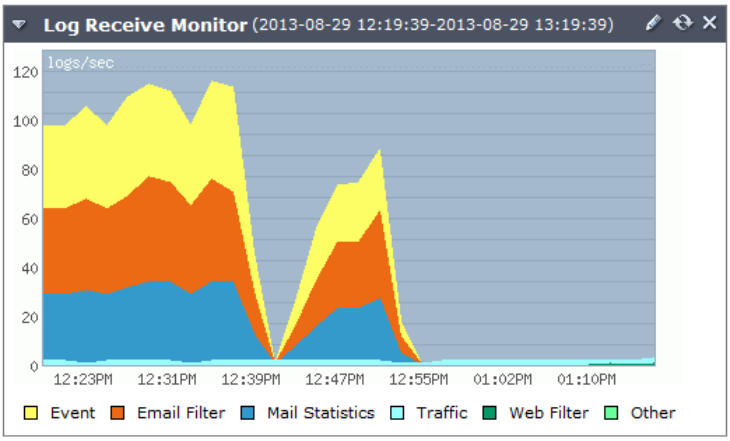
The following settings can be configured:

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 time ranges: *Last 10 Minutes*, *Last 1 Hour,* or *Last 24 Hours*.
Refresh Interval	Automatically refresh the widget. Enter a number between 10 and 240 seconds. To disable automatic refresh, enter `0`.

Log Receive Monitor widget

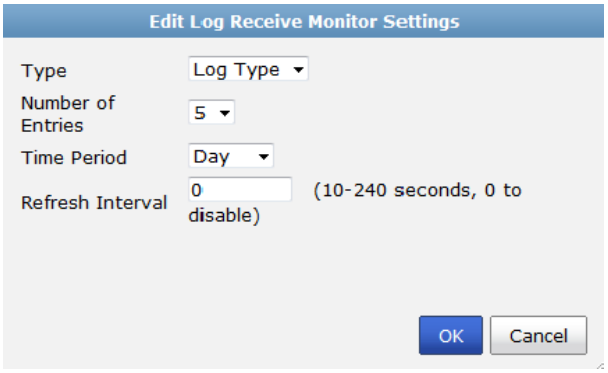
The *Log Receive Monitor* widget displays the rate at which logs are received over time. You can select to display log data by log type or per device.

Figure 50: Log receive monitor widget (log type)



To configure settings for the widget, select *Edit* from the title bar.

Figure 51: Edit log receive monitor settings



Configure the following settings:

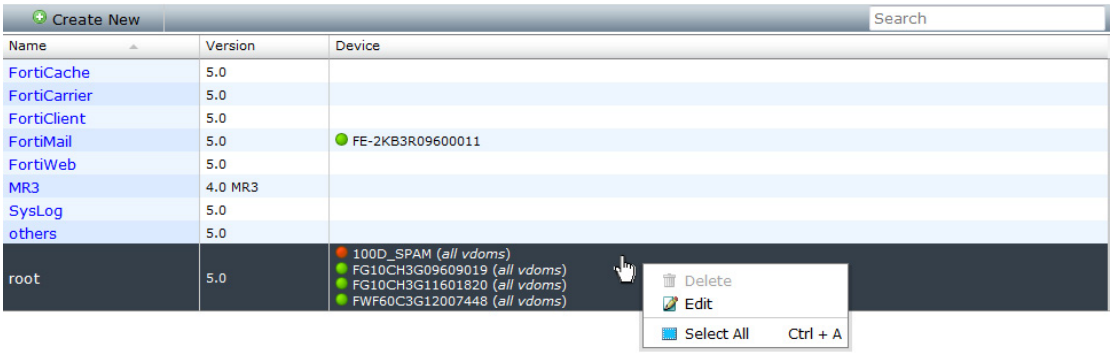
Type	From the drop-down menu, select either: • *Log Type*: Display the type of logs that are received from all registered devices separated into the following categories: *Event, Email Filter, Mail Statistics, Traffic, Web Filter*, and *Other*. • *Device*: Display the logs that received by each registered device separated into the top number of devices.
Number of Entries	Select the number of either log types or devices shown in the widget's graph.
Time Period	Select one of the following time ranges over which to monitor the rate at which log messages are received: *Hour*, Day, *Week*.
Refresh Interval	Automatically refresh the widget. Enter a number between 10 and 240 seconds. To disable automatic refresh, enter `0`.

All ADOMs

The *All ADOMs* menu item displays all the ADOMs configured on the device, and provides the option to create new ADOMs. It is only visible if ADOMs are enabled, see "System Information widget" on page 60.

FortiAnalyzer v5.0 Patch Release 3 or later supports FortiGate, FortiCache, FortiCarrier, FortiClient, FortiMail, FortiWeb, and other ADOM types.

Figure 52: All ADOMs list



The following information and options are available:

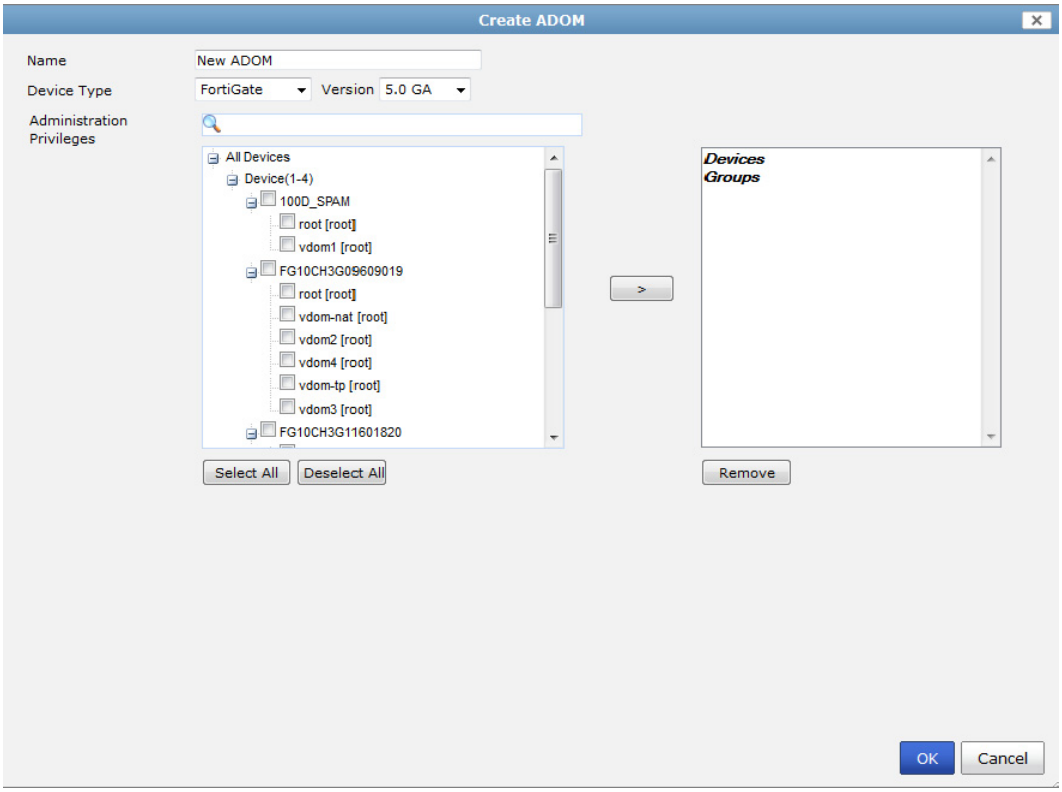
Create New	Select to create a new ADOM. See "To create a new ADOM:" on page 76.
Search	Enter a keyword to search your ADOMs.
Name	The names of the current ADOMs.
Version	The firmware release version of the ADOM.
Device	The devices currently in the ADOM.
Delete	Select *Delete* in the right-click menu to delete the ADOM.
Edit	Select *Edit* in the right-click menu to edit the ADOM.
Select All	Select *Select All* in the right-click menu to select all ADOMs in the list. Alternatively, you can use CTRL + A to select all the ADOMs.

To create a new ADOM:

1. Select *Create New* from the ADOM list toolbar, or right-click in the ADOM list and select *New* in the right-click menu.

   The *Create ADOM* dialog box opens.

   Figure 53: Create a new ADOM



2. Enter a name for the ADOM in the *Name* field.
3. Select the device type and firmware version from the drop-down lists.
4. Select the devices to be added to the ADOM from the device list on the left, then select the arrow button to transfer them into the selected devices list on the right.
5. Select *OK* to create the ADOM.

To edit an ADOM:

1. Right-click on the ADOM you need to edit and select *Edit* from the right-click menu.

   The *Edit ADOM* dialog box opens.

2. Edit the ADOM information as required and then select *OK*.

   The device type and version cannot be edited.

The default ADOMs cannot be edited.

To disable an ADOM:

1. Right-click on the ADOM you need to edit and select *Edit* from the right-click menu.

   The *Edit ADOM* dialog box opens.
2. Uncheck the *Status* checkbox and then select *OK*.

   You must remove all devices before disabling the ADOM.

The default ADOMs cannot be disabled.

To delete an ADOM:

1. Right-click on the ADOM you would like to delete and select *Delete* from the right-click menu.
2. Select *OK* in the confirmation dialog box to delete the ADOM.

The default ADOMs cannot be deleted.

RAID Management

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

This menu is only available on devices that support RAID.

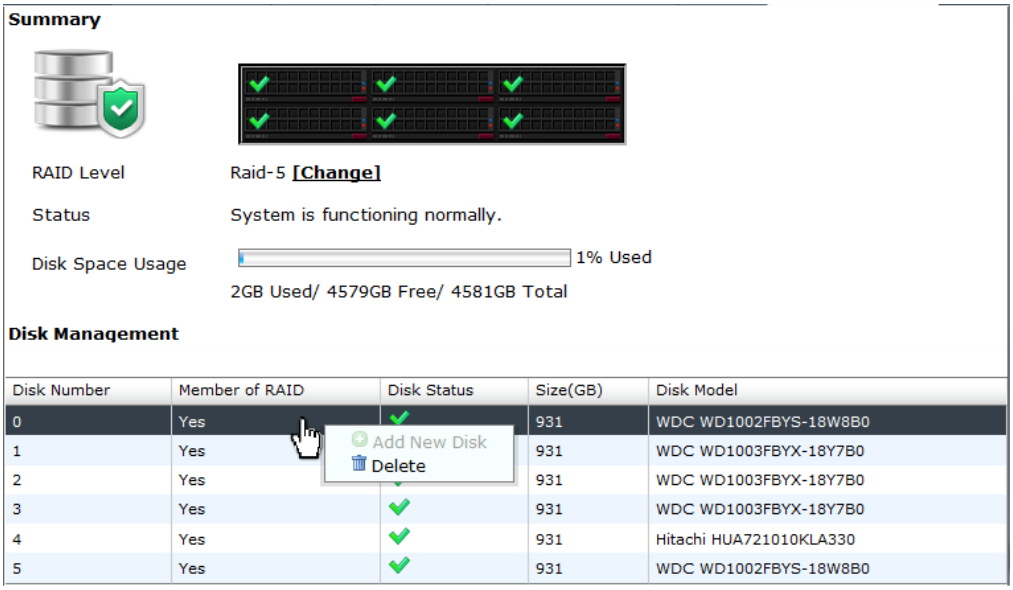
You can view the status of the RAID array from the RAID menu in *System Settings* > *RAID Management*. The RAID Management page displays the status of each disk in the RAID array, including the disk's RAID level. This menu also displays how much disk space is being used.

Under *Disk Management* the following information is displayed: *Disk Number*, *Member of RAID*, *Disk Status*, *Size (GB)*, and *Disk Model*. See Figure 54 on page 78.

The *Alert Message Console* widget, located in *System Settings*> *Dashboard*, will provides detailed information about any RAID array failures. For more information see "Alert Messages Console widget" on page 70.

If you need to remove a disk from the FortiAnalyzer unit, you might be able to hot swap it. Hot swapping means that you remove a failed hard disk and replace it with a new one while the FortiAnalyzer unit is in operation. Hot swapping is a quick and efficient way to replace hard disks. For more information about hot swapping, see "Hot swapping hard disks" on page 82.

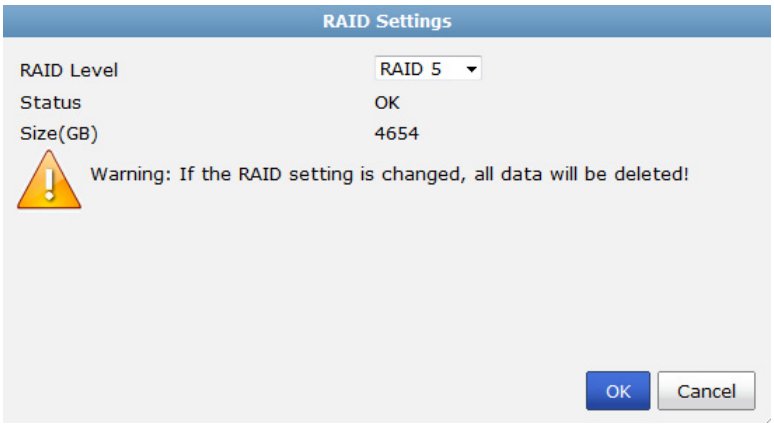
Figure 54:RAID Management menu page



To configure the RAID level:

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

   Figure 55:RAID settings dialog box



2. From the *RAID Level* drop-down list, select the RAID level you want to use, then select *OK*.
   Once selected, depending on the RAID level, it may take a significant amount of time to generate the RAID array.

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

Supported RAID levels

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

- ***Linear***

  Linear RAID 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 FortiAnalyzer 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 FortiAnalyzer unit can distribute disk writing across multiple disks.

  Minimum number of drives: 2

  Data protection: No protection

RAID 0 is not recommended for mission critical environments as it is not fault-tolerant.

- ***RAID 1***

  A RAID 1 array is also referred to as mirroring. The FortiAnalyzer unit writes information to one hard disk, and writes a copy (a mirror image) of all information to all the 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 backup hard disks available.

  Minimum number of drives: 2

  Data protection: Single-drive failure

One write or two reads are possible per mirrored pair. RAID 1 offers redundancy of data. A re-build is not required in the event of a drive failure. This is the simplest RAID storage design with the highest disk overhead.

- ***RAID 1 +Spare***

  A RAID 1 with hot spare (or RAID 1s) 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 becomes the new hot spare.

- ***RAID 5***

  A RAID 5 array employs striping with a parity check. Similar to RAID 0, the FortiAnalyzer 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 FortiAnalyzer unit will restore the data on the new disk by using reference information from the parity volume.

Minimum number of drives: 3

Data protection: Single-drive failure

- ***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 becomes the new hot spare.

- ***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.

  Minimum number of drives: 4

  Data protection: Up to two disk failures.

- ***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.

  Minimum number of drives: 4

  Data protection: Up to two disk failures in each sub-array.

Alternative to RAID 1 when additional performance is required.

- ***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.

  Minimum number of drives: 6

  Data protection: Up to one disk failure in each sub-array.

Higher fault tolerance than RAID 5 and higher efficiency than RAID 0.

- ***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.

  Minimum number of drives: 8

  Data protection: Up to two disk failures in each sub-array.

High read data transaction rate, medium write data transaction rate, and slightly lower performance than RAID 50.

RAID support per FortiAnalyzer model

Table 3: RAID support per FortiAnalyzer model

Model	RAID Type	RAID Level	Hot Swappable
FAZ-100C	-	-	-
FAZ-200D	-	-	-
FAZ-300D	Software RAID	Linear, 0, 1	No
FAZ-400B	Software RAID	0, 1	No
FAZ-400C	-	-	-
FAZ-1000B	Software RAID	1	No
FAZ-1000C	Software RAID	Linear, 0, 1, 10	No
FAZ-1000D	Software RAID	Linear, 0, 1, 10	No
FAZ-2000A	Hardware RAID	0, 5, 5 + Spare, 10, 50	Yes
FAZ-2000B	Hardware RAID	0, 5, 5 +Spare, 6, 6 +Spare, 10, 50	Yes
FAZ-3000D	Hardware RAID	0, 1, 1 +Spare, 5, 5 +Spare, 6, 6 +Spare, 10, 50, 60	Yes

Table 3: RAID support per FortiAnalyzer model (continued)

Model	RAID Type	RAID Level	Hot Swappable
FAZ-4000A	Hardware RAID	0, 5, 5 +Spare, 10, 50	Yes
FAZ-4000B	Hardware RAID	0, 5, 5 +Spare, 6, 6 +Spare, 10, 50, 60	Yes
FAZ-VM	-	-	-
FAZ-VM64, FAZ-VM64-HV	-	-	-

RAID disk status

The RAID management page displays the status of each disk in the RAID array. The possible disk states are:

- *OK*: The hard drive is functioning normally.
- *Rebuilding*: The FortiAnalyzer unit is writing data to a newly added hard drive in order to restore the hard drive to an optimal state. The FortiAnalyzer unit is not fully fault tolerant until rebuilding is complete.
- *Initializing*: The FortiAnalyzer unit is writing to all the hard drives in the device in order to make the array fault tolerant.
- *Verifying*: The FortiAnalyzer unit is ensuring that the parity data of a redundant drive is valid.
- *Degraded*: The hard drive is no longer being used by the RAID controller.
- *Inoperable*: One or more drives are missing from the FortiAnalyzer unit. The drive is no longer available to the operating system. Data on an inoperable drive cannot be accessed.

Hot swapping hard disks

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

To identify which hard disk failed, read the relevant log message in the *Alert Message Console* widget (see “Alert Messages Console widget” on page 70).

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 FortiAnalyzer 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 FortiAnalyzer 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 FortiAnalyzer 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 FortiAnalyzer unit will automatically add the new disk to the current RAID array. The status appears on the console. The RAID management 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 FortiAnalyzer unit.

Adding new disks

Some FortiAnalyzer 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 FortiAnalyzer unit. You can also migrate the data to another FortiAnalyzer 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 64.
3. If your device has hardware RAID, install the disks in the FortiAnalyzer unit while the FortiAnalyzer unit is running.

   If your device has software RAID, shutdown the device (see “Shutdown” on page 67), install the disk or disks, then restart the device.
4. Configure the RAID level.

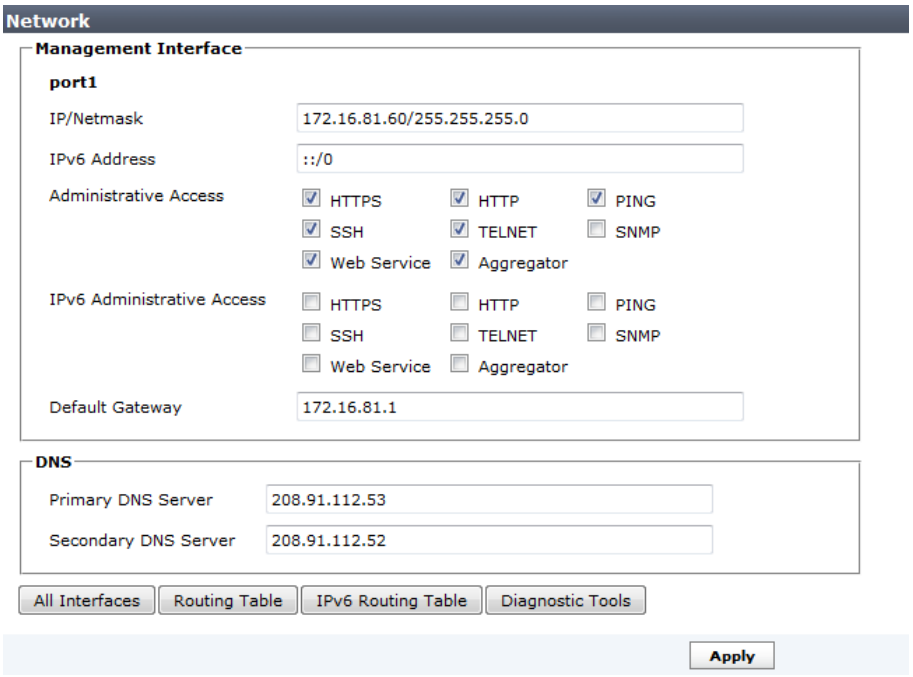
   If you have backed up the log data, restore the data. For more information, see “Restoring the configuration” on page 65.

Network

The FortiAnalyzer unit can manage Fortinet devices connected to any of its interfaces. The DNS servers must be on the networks to which the FortiAnalyzer unit connects, and should have two different addresses.

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

Figure 56: Network page



Configure the following settings:

Management Interface	
IP/Netmask	The IP address and netmask associated with this interface.
IPv6 Address	The IPv6 address and netmask associated with this interface.
Administrative Access	Select the allowed administrative service protocols from: *HTTPS*, *HTTP*, *PING*, *SSH*, *TELNET*, *SNMP*, *Web Service*, and *Aggregator*.
IPv6 Administrative Access	Select the allowed IPv6 administrative service protocols from: *HTTPS*, *HTTP*, *PING*, *SSH*, *TELNET*, *SNMP*, *Web Service*, and *Aggregator*.
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 “Network interfaces” on page 85.
Routing Table	Click to open the routing table. See “Static routes” on page 87.
IPv6 Routing Table	Click to open the IPv6 routing table. See “IPv6 static routes” on page 88.
Diagnostic Tools	Select to run available diagnostic tools, including *Ping*, *Traceroute*, and *View logs*. See “Diagnostic tools” on page 89.

Network interfaces

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

Figure 57: Network interface list

Name	IP/Netmask	IPv6 Address	Description	Administrative Access	IPv6 Administrative Access	Enable
port1	172.16.81.80 / 255.255.255.0	::/0		HTTPS, HTTP, PING, SSH, TELNET, SNMP, Web Service	HTTPS	
port2	0.0.0.0 / 0.0.0.0	::/0				
port3	0.0.0.0 / 0.0.0.0	::/0				
port4	0.0.0.0 / 0.0.0.0	::/0				

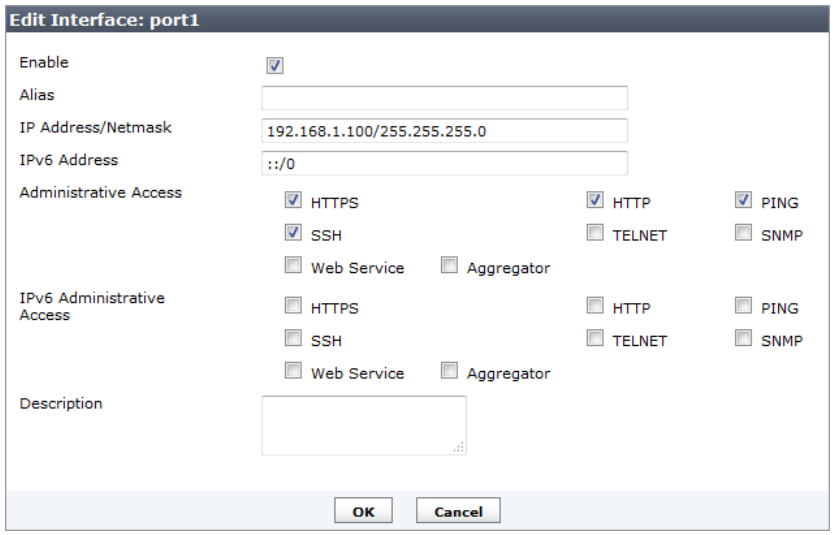
The following information is available:

Name	The names of the physical interfaces on your FortiAnalyzer unit. The name 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 86. 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.
IPV6 Administrative access	The list of allowed IPv6 administrative service protocols on this interface.
Enable	Displays if the interface is enabled (green circle with a check mark) or disabled (gray circle with an X).

Configuring network interfaces

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

Figure 58: Configure network interfaces



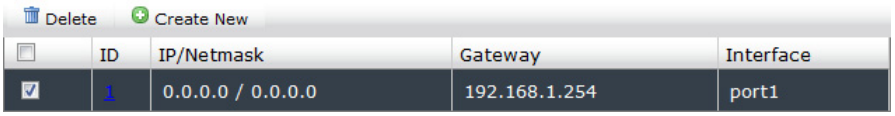
Configure the following settings:

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

Static routes

Go to *System Settings* > *Network* and select the *Routing Table* button to view, edit, or add to the static routing table.

Figure 59: Routing table



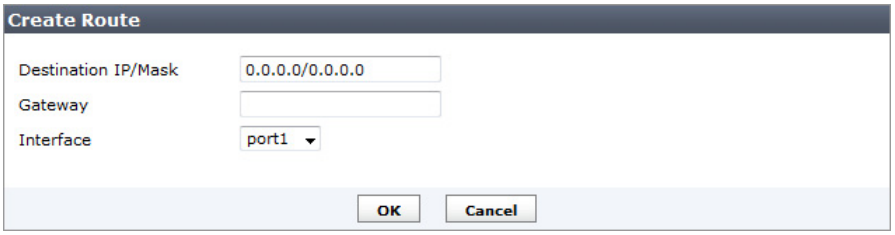
The following information/options are available:

Delete	Select the check box next to the route number then 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 87.
ID	The route number. Select it to edit the route settings.
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 60: Create new route



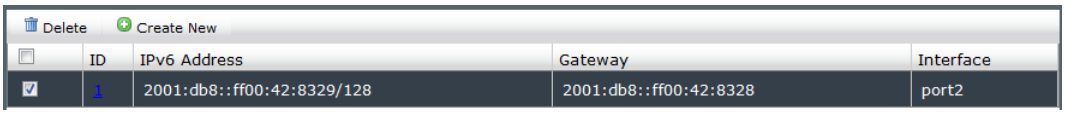
Configure the following settings, then select *OK* to create the new static route:

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

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.

Figure 61:IPv6 routing table



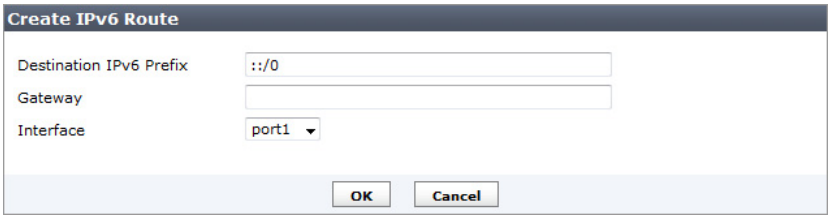
The following information and settings are available:

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 88.
ID	The route number. Select it to edit the route settings.
IPv6 Address	The destination IPv6 address for this route.
Gateway	The IPv6 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 62: Create new route



Configure the following settings, then select *OK* to create the new IPv6 static route:

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

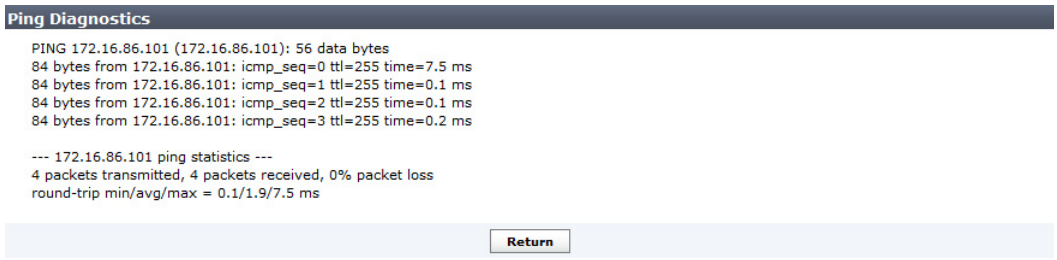
Diagnostic tools

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

Figure 63: Diagnostic tools

Figure 64 provides an example Ping diagnostic output of an internal network device.

Figure 64: Example Ping diagnostics output



Admin

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

Administrator	Select to configure administrative users accounts. For more information, see “Administrator” on page 91.
Profile	Select to set up access profiles for the administrative users. For more information, see “Profile” on page 95.
Remote Auth Server	Select to configure authentication server settings for administrative log in. For more information, see “Remote authentication server” on page 99.
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 104.

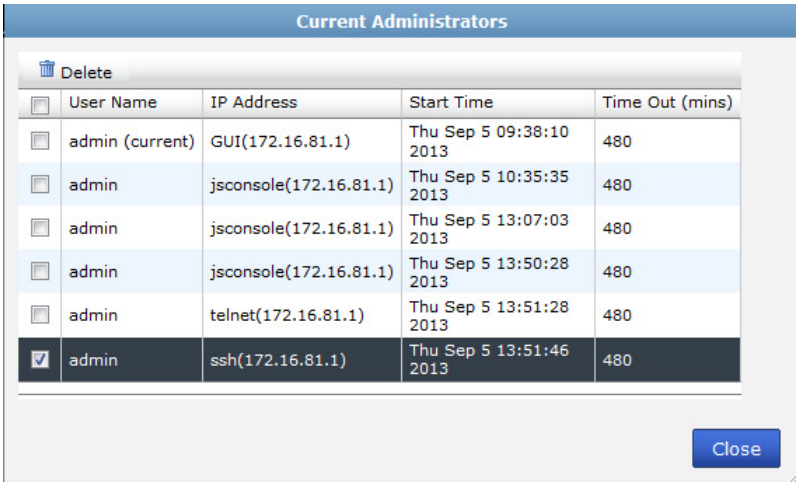
Monitoring administrator sessions

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

To view logged in administrators on the FortiAnalyzer unit, go to *System Settings* > *Dashboard.* In the *System Information* widget, under *Current Administrators*, select *Detail*.

The list of current administrator sessions opens.

Figure 65: 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 login type (GUI, jsconsole, SSH, telnet) and IP address where the administrator is logging in from.
Start Time	The date and time the administrator logged in.
Time Out (mins)	The maximum duration of the session in minutes (1 to 480 minutes).
Delete	Select the check box next to the user and select *Delete* to drop their connection to the FortiAnalyzer unit.

To disconnect an administrator:

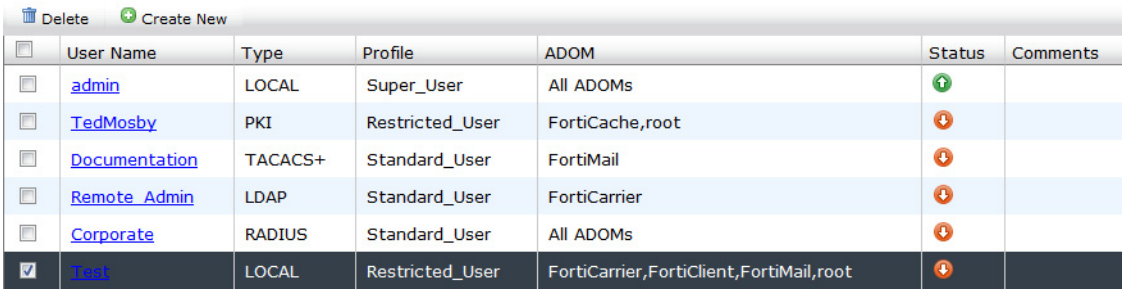
1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Current Administrators field*, select *Detail*. The list of current administrator sessions appears; see Figure 65.
3. Select the check box for each administrator session that you want to disconnect, and select *Delete*.
4. Select *OK* to confirm deletion of the session.

   The disconnected administrator will see the FortiAnalyzer login screen when disconnected. They will not have any additional warning. If possible, it is advisable to inform the administrator before disconnecting them, in case they are in the middle of important configurations for the FortiAnalyzer 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 66: Administrator list



The following information is available:

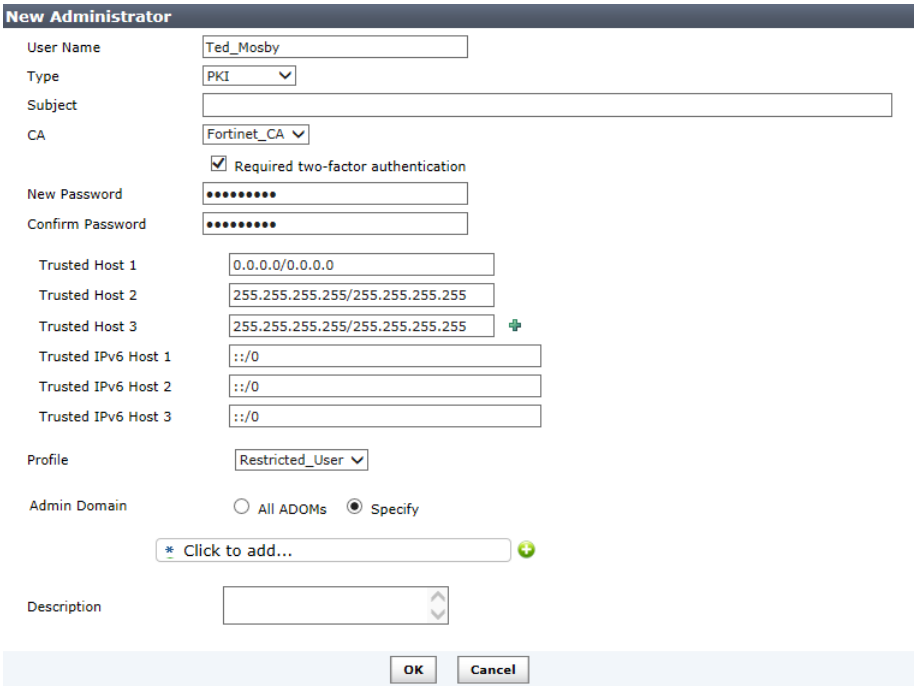
Delete	Select the check box next to the administrator you want to remove from the list and select *Delete*.
Create New	Select to create a new administrator. For more information, see "To create a new administrator account:" on page 92.
User Name	The name this administrator uses to log in. Select the administrator name to edit the administrator settings.
Type	The type of administrator account, one of: *LOCAL, RADIUS, LDAP, TACACS+*, or *PKI*.
Profile	The administrator profile for this user that determines the privileges of this administrator. The profile can be one of: *Restricted_User*, *Standard_User*, *Super_User*, or a custom defined profile. For information on administrator profiles, see "Profile" on page 95.
Admin Domain	The ADOMs to which the user has access. ADOM access can be to all ADOMs or specific ADOMs which are assigned to the profile.
Status	Indicates whether the administrator is currently logged into the FortiAnalyzer unit not. A green circle with an up arrow indicates that the administrator is logged in, a red circle with a down arrow indicates that they are not.
Comments	Descriptive text about the administrator account.

To create a new administrator account:

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

   The *New Administrator* dialog box appears.

Figure 67: New administrator dialog box



2. Configure the following settings:

User Name	Enter the name that this administrator uses to log in.
Type	Select the type of authentication the administrator will use when logging into the FortiAnalyzer unit. Select one of: *LOCAL*, *RADIUS*, *LDAP*, *TACACS+*, or *PKI*. If you select *LOCAL*, you will need to add a password.
Subject	If *Type* is set to *PKI*, enter a description.
CA	If *Type* is set to *PKI*, select a certificate in the drop-down list.
Require two-factor authentication	If *Type* is set to *PKI*, you can select the checkbox to enforce two-factor authentication. Enter a password and confirm.
New Password	Enter the password.
Confirm Password	Enter the password again to confirm it.
Server	Select the RADIUS, LDAP, or TACACS+ server, as appropriate. This option is only available if *Type* is not *LOCAL* or *PKI*.
wildcard	Select this option to set the password as a wildcard. This option is only available if *Type* is not *LOCAL* or *PKI*.

Trusted Host1 **Trusted Host2** **Trusted Host3** **...**	Optionally, enter the trusted host IP address and network mask from which the administrator can log in to the FortiAnalyzer unit. You can specify up to ten trusted hosts in the Web-based Manager or in the CLI. Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see "Using trusted hosts" on page 95.
Trusted IPv6 Host1 **Trusted IPv6 Host2** **Trusted IPv6 Host3** **...**	Optionally, enter the trusted host IPv6 address from which the administrator can log in to the FortiAnalyzer unit. You can specify up to three trusted IPv6 hosts in the Web-based Manager. You can configure up to ten trusted hosts in the CLI. 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 95.
Profile	Select a profile from the list. The profile selected determines the administrator's access to the FortiAnalyzer unit's features. To create a new profile see "Configuring administrator profiles" on page 98.
Admin Domain	Choose the ADOM this admin will belong to. This field is available only if ADOMs are enabled (see "Administrative Domains" on page 38). Select either *All ADOMs* or *Specify*. When selecting *Specify*, select the plus (+) icon to the left of the field to select one or multiple ADOMs. The *Super_User* profile defaults to *All ADOMs* access.
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.

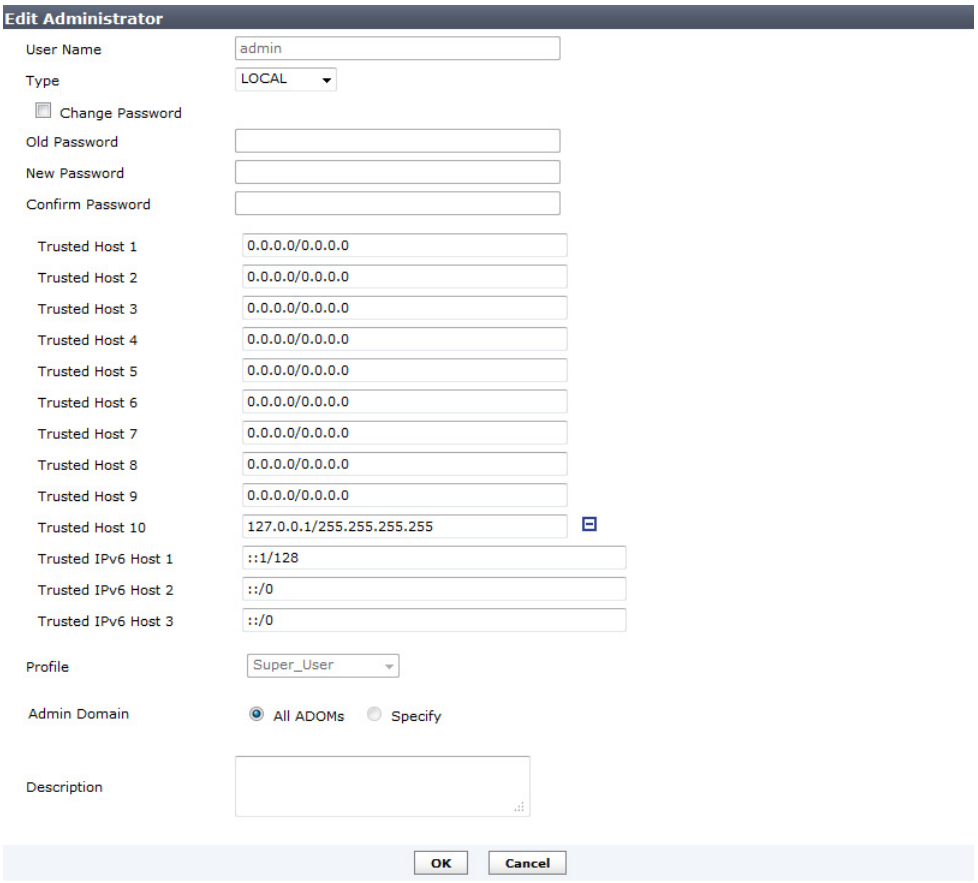
3. Select *OK* to create the new administrator account.

To modify an existing administrator account:

1. Go to *System Settings* > *Admin* > *Administrator.* The list of configured administrators appears; see Figure 66 on page 91.
2. In the *User Name* column, click on the user name of the administrator you want to change.

   The *Edit Administrator* window appears.

Figure 68: Edit administrator page



3. Modify the settings as required. For more information about configuring account settings, see "To create a new administrator account:" on page 92.
4. Select *OK* to save your changes.

To delete an existing administrator account:

The default *admin* administrator account cannot be deleted.

1. Go to *System Settings* > *Admin* > *Administrator.* The list of configured administrators appears; see Figure 66 on page 91.
2. Select the check box of the administrator account you want to delete and then select the *Delete* icon in the toolbar.
3. Select *OK* in the confirmation dialog box to delete the administrator account.

Using trusted hosts

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

When you set trusted hosts for all administrators, the FortiAnalyzer 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 that are used to limit administrator access privileges to devices or system features. There are three predefined 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.

Table 4 lists permissions for the three predefined administrator profiles. When *Read-Write* is selected, the user can view and make changes to the FortiAnalyzer system. When *Read-Only* is selected, the user can only view information. When *None* is selected, the user can neither view or make changes to the FortiAnalyzer system. The administrator profile restricts access to both the FortiAnalyzer Web-based Manager and CLI.

Table 4: Predefined profiles, FortiAnalyzer features, and permissions

Feature	Predefined Administrator Profiles		
	Super User	**Standard User**	**Restricted User**
System Settings / `system-setting`	Read-Write	None	None
Administrator Domain / `adom-switch`	Read-Write	Read-Write	None
Device Manager / `device-manager`	Read-Write	Read-Write	Read-Only
Add/Delete Devices/Groups / `device-op`	Read-Write	Read-Write	None
Drill Down / `realtime-monitor`	Read-Write	Read-Write	Read-Only

Table 4: Predefined profiles, FortiAnalyzer features, and permissions (continued)

Feature	Predefined Administrator Profiles		
	Super User	**Standard User**	**Restricted User**
Log View / `log-viewer`	Read-Write	Read-Write	Read-Only
Reports / `report-viewer`	Read-Write	Read-Write	Read-Only
Event Management / `event-management`	Read-Write	Read-Write	Read-Only
CLI Only Settings			
profileid	Super_User	Standard_User	Restricted_User
scope	global	global	global
global-policy-packages	Not in use.	Not in use.	Not in use.
global-objects	Not in use.	Not in use.	Not in use.
assignment	Not in use.	Not in use.	Not in use.
read-passwd	Not in use.	Not in use.	Not in use.
device-config	Not in use.	Not in use.	Not in use.
device-profile	Not in use.	Not in use.	Not in use.
policy-objects	Not in use.	Not in use.	Not in use.
deploy-management	Not in use.	Not in use.	Not in use.
config-retrieve	Not in use.	Not in use.	Not in use.
term-access	Not in use.	Not in use.	Not in use.
adom-policy-packages	Not in use.	Not in use.	Not in use.
adom-policy-objects	Not in use.	Not in use.	Not in use.
vpn-manager	Not in use.	Not in use.	Not in use.
consistency-check	Not in use.	Not in use.	Not in use.
faz-management	Not in use.	Not in use.	Not in use.
fgd_center	Not in use.	Not in use.	Not in use.
network	Not in use.	Not in use.	Not in use.
admin	Not in use.	Not in use.	Not in use.
system	Not in use.	Not in use.	Not in use.
devices	Not in use.	Not in use.	Not in use.
alerts	Not in use.	Not in use.	Not in use.
dlp	Not in use.	Not in use.	Not in use.

Table 4: Predefined profiles, FortiAnalyzer features, and permissions (continued)

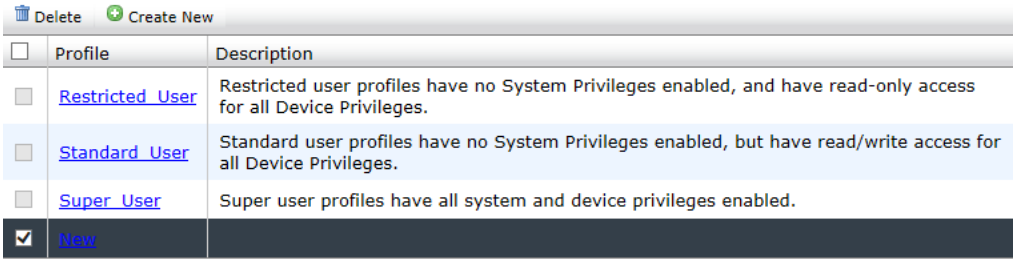
Feature	Predefined Administrator Profiles		
	Super User	**Standard User**	**Restricted User**
reports	Not in use.	Not in use.	Not in use.
logs	Not in use.	Not in use.	Not in use.
quar	Not in use.	Not in use.	Not in use.
net-monitor	Not in use.	Not in use.	Not in use.
vuln-mgmt	Not in use.	Not in use.	Not in use.

You cannot delete these profiles, but you can modify them. You can also create new profiles if required, see "Configuring administrator profiles" on page 98.

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 69: Administrator profile list



The default administrator profiles cannot be edited or deleted.

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 98.

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 98.
Description	Provides a brief description of the system and device access privileges allowed for the selected profile.

Configuring administrator profiles

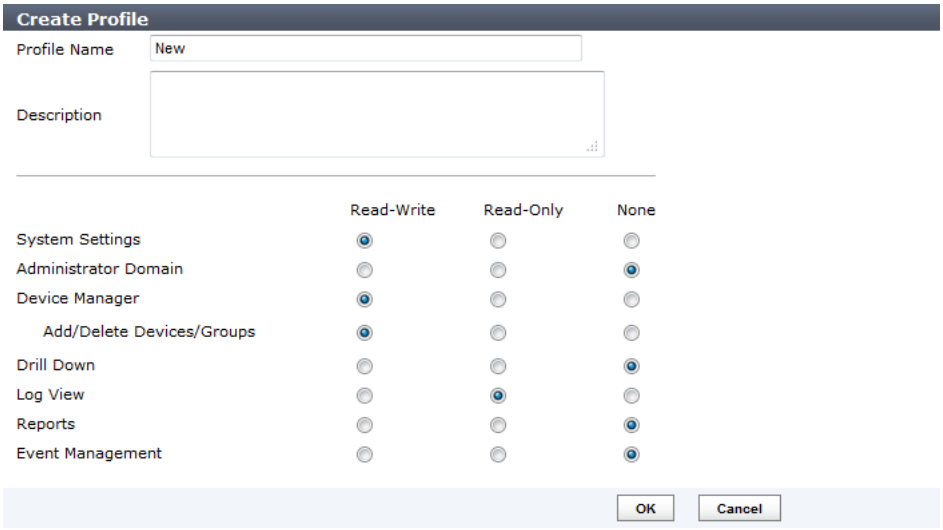
You can modify one of the predefined profiles or create a custom profile if needed. Only administrators with full system privileges can modify the administrator profiles.

To create a custom profile:

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

   The *Create Profile* dialog box opens.

   Figure 70: 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.
Other Settings	Select *None*, *Read Only*, or *Read-Write* access for categories as required.

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

To modify an existing profile:

1. Go to *System Settings* > *Admin* > *Profile*. The list of available profiles appears; see Figure 69 on page 97.
2. In the *Profile* column, click on the name of the profile you want to change. The *Edit Profile* dialog box appears.

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

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

The Name field cannot be changed when editing the profile in the Web-based Manager.

To delete a profile:

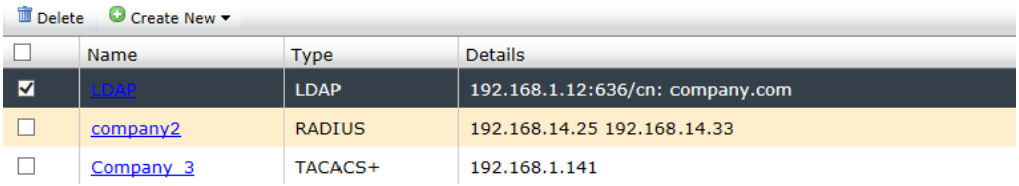
1. Go to *System Settings* > *Admin* > *Profile*. The list of available profiles appears; see Figure 69 on page 97.
2. Select the check box of the custom profile you want to delete and then select the *Delete* icon in the toolbar. You can only delete custom profiles when they are not applied to any administrators.
3. Select *OK* in the confirmation dialog box to delete the profile.

Remote authentication server

The FortiAnalyzer system supports remote authentication of administrators using RADIUS, LDAP, and TACACS+ servers. To use this feature, you must configure the appropriate server entries in the FortiAnalyzer unit for each authentication server in your network.

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

Figure 71: Server list



The following information/options are available:

Create New	Add a new LDAP, RADIUS, or TACACS+ server entry.
Delete	Select the check box next to the server entry and select *Delete*. You cannot delete a server entry if there are administrator accounts using it.
Name	The server name. Select the server name to edit the settings.

Type	The type of server, either LDAP, RADIUS, or TACACS+.
Details	The IP address or DNS resolvable domain name of the server.

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 appears, depending on the server type selected.
3. Modify the settings as required and select *OK* to apply your changes.

The *Name* field cannot be changed when editing a server configuration in the Web-based Manager.

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. A confirmation dialog box appears.
3. Select *OK* to delete the server entry.

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

LDAP server

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

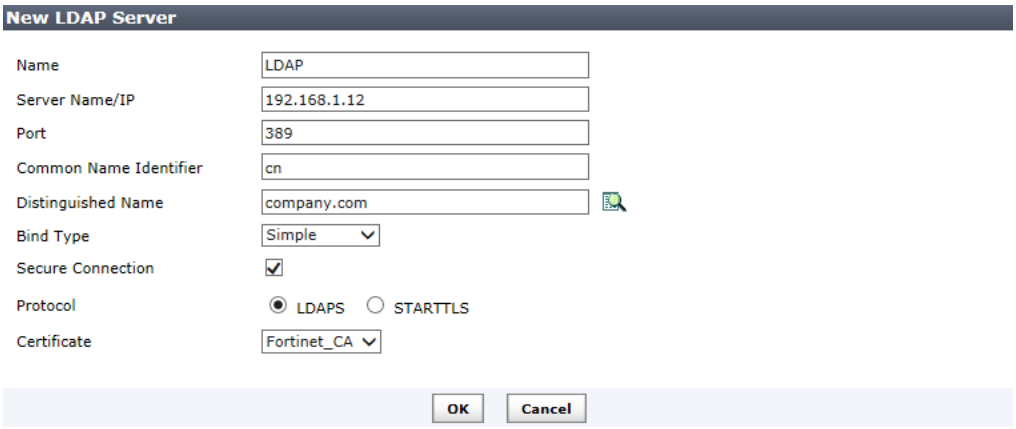
If you have configured LDAP support and require a user to authenticate using an LDAP server, the FortiAnalyzer unit contacts the LDAP server for authentication. To authenticate with the FortiAnalyzer unit, the user enters a user name and password. The FortiAnalyzer unit sends this user name and password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

To add a LDAP server:

1. Go to *System Settings* > *Admin* > *Remote Auth Server*.
2. Select the *Create New* toolbar and select LDAP in the drop-down list.

   The *New LDAP Server* dialog box opens.

Figure 72: 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.
Bind Type	Select the type of binding for LDAP authentication from the drop-down list. One of: *Simple*, *Anonymous*, or *Regular*.
User DN	Enter the user distinguished name. This option is available when the *Bind Type* is set to *Regular*.
Password	Enter the user password. This option is available when the *Bind Type* is set to *Regular*.
Secure Connection	Select to use a secure LDAP server connection for authentication.
Protocol	Select either LDAPS or STARTTLS in the protocol field.
Certificate	Select the certificate in the drop-down list.

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

RADIUS server

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

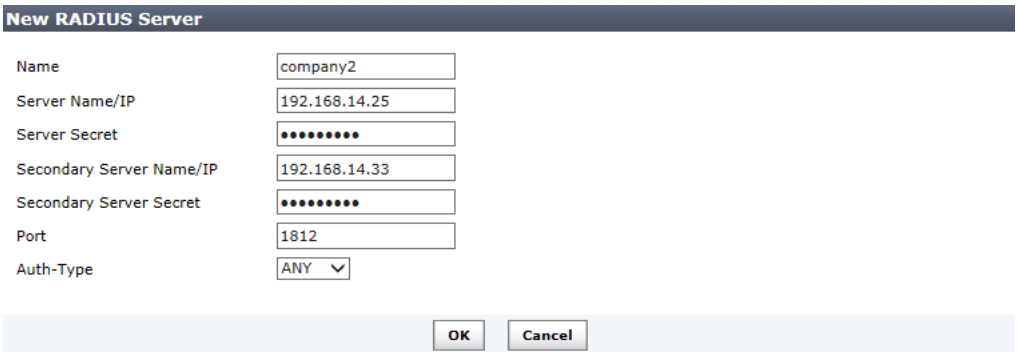
You can create or edit RADIUS server entries in the RADIUS server list to support authentication of administrators. When an administrator account's type is set to RADIUS, the FortiAnalyzer unit uses the RADIUS server to verify the administrator password at logon. The password is not stored on the FortiAnalyzer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

To add a RADIUS server configuration:

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

   The *New RADIUS Server* dialog box appears.

Figure 73: 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. Some RADIUS servers use port 1645.
Auth-Type	Enter the authentication type the RADIUS server requires. Select from *ANY, PAP, CHAP*, or *MSv2 (MSCHAPv2)*. The default setting of *ANY* has the FortiAnalyzer unit try all the authentication types.

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

TACACS+ server

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.

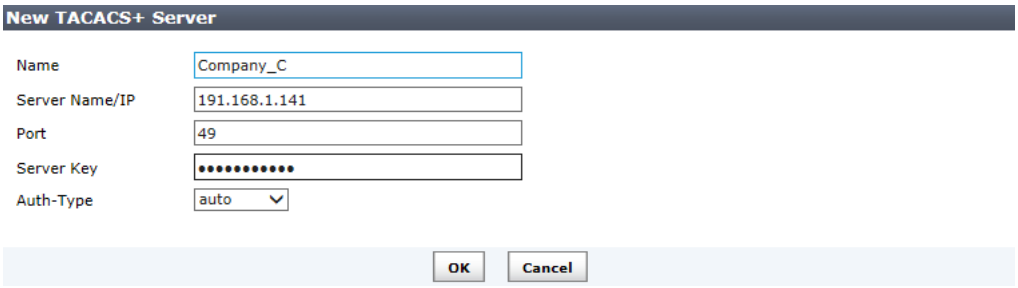
For more information about TACACS+ servers, see the FortiGate documentation.

To add a TACACS+ server:

1. Go to *System Settings* > *Admin* > *Remote Auth Server*.
2. Select the *Create New* toolbar icon.

   The *New TACACS+ Server* dialog box appears.

Figure 74: 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 *49*.
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. Select one of: *auto, ASCII, PAP, CHAP,* or *MSCHAP*. The default value is *auto*.

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

Administrator settings

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

- Ports for HTTPS and HTTP administrative access
- HTTPS & Web Service server certificate
- Idle Timeout settings
- Language of the web-based manager
- Password Policy

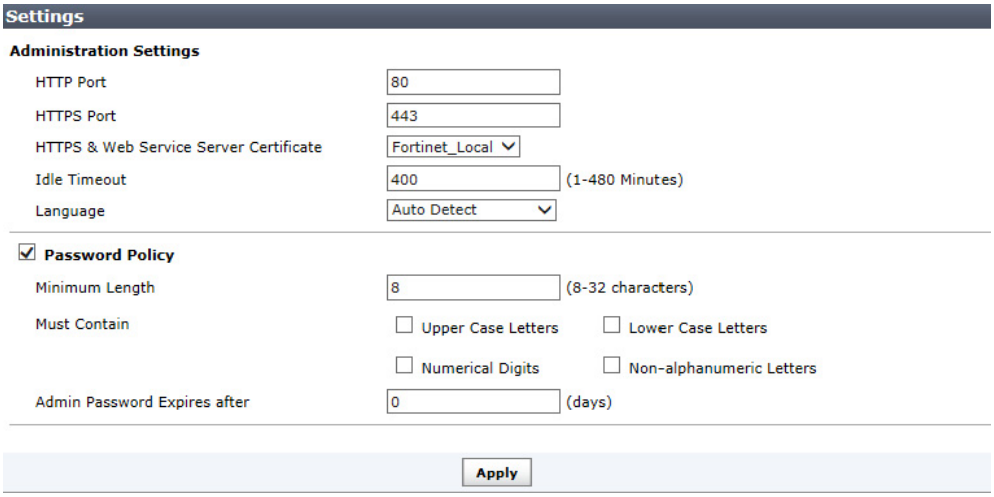
Only the `admin` administrator can configure these system options, which apply to all administrators logging onto the FortiAnalyzer unit.

To configure the administrative settings:

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

   The *Settings* dialog box opens.

   Figure 75: Settings dialog box



2. Configure the following settings:

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 FortiAnalyzer unit, creating the possibility of someone walking up and modifying the network options.

Language	Select a language from the drop-down list. Select either *English, Simplified Chinese, Traditional Chinese, Japanese, Korean*, or *Auto Detect*. The default value is *Auto Detect*.
Password Policy	
Enable	Select to enable administrator passwords.
Minimum Length	Select the minimum length for a password. The default is eight characters.
Must Contain	Select the types of characters that a password must contain.
Admin Password Expires after	Select the number of days that a password is valid for, after which time it must be changed.

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

Certificates

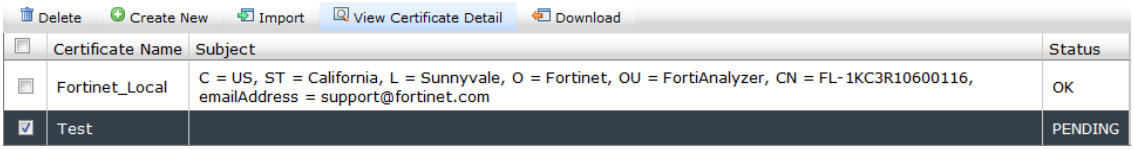
The FortiAnalyzer unit generates a certificate request based on the information you enter to identify the FortiAnalyzer unit. After you generate a certificate request, you can download the request to a computer that has management access to the FortiAnalyzer unit and then forward the request to a CA.

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

Local certificates

The FortiAnalyzer has one default local certificate, *Fortinet_Local*. From this menu you can create, delete, import, view, and download local certificates.

Figure 76: Local certificates sub-menu

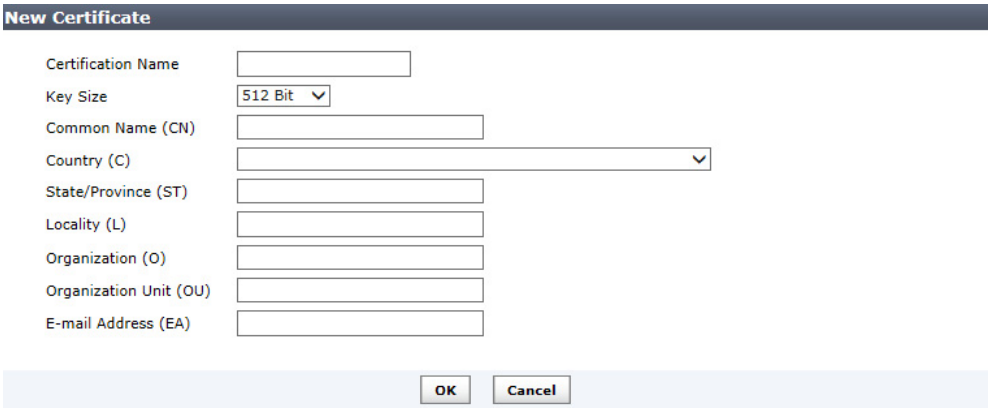


To create a local certificate request:

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

   The *New Certificate* window opens.

Figure 77: New local certificate



3. Configure the following settings:

Certificate Name	The name of the certificate.
Key Size	Select the key size from the drop-down list. Select one of: *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 setting. The request is sent and the status is listed as pending.

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

To import a local certificate:

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

   The *Import* dialog box opens.
3. Select *Choose File*, browse to the location of the certificate, and select *OK*.

To view a local certificate:

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

   The *Result* page opens.

Figure 78: Result page

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 return to the local certificates list.

To download a local certificate:

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

To delete a local certificate:

1. Go to *System Settings* > *Certificates* > *Local Certificates*.
2. Select the certificate or certificates that you would like to delete and select *Delete*.
3. Select *OK* in the confirmation dialog box to delete the certificate.

CA certificates

The FortiAnalyzer has one default CA certificate, Fortinet_CA. In this sub-menu you can:

- Delete CA certificates
- Import CA certificates
- View certificate details
- Download CA certificates

To import a CA certificate:

1. Go to *System Settings* > *Certificates* > *CA Certificates*.
2. Select the *Import* button.

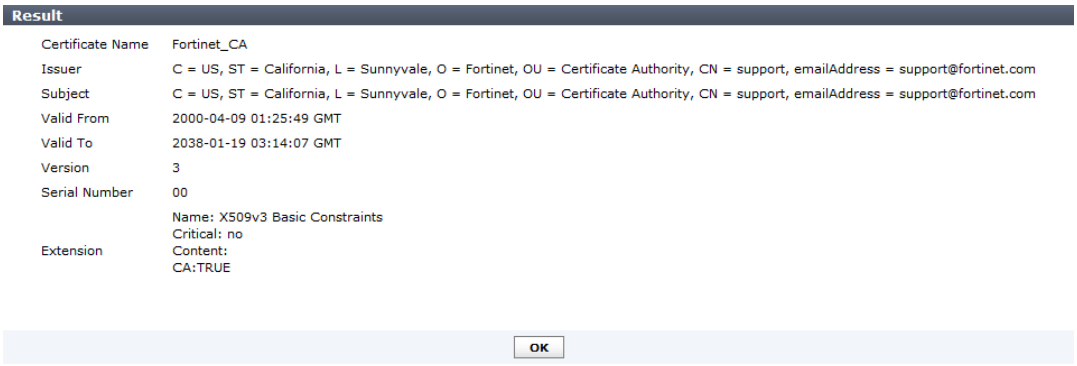
   The *Import* dialog box opens.
3. Select *Choose File*, browse to the location of the certificate, and select *OK*.

To view a CA certificate:

1. Go to *System Settings* > *Certificates* > *CA Certificates*.
2. Select the certificates that you would like to see details about, then select *View Certificate Detail*.

   The *Result* page opens.

Figure 79: Result page



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 return to the CA certificates list.

To download a CA certificate:

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

To delete a CA certificate:

1. Go to *System Settings* > *Certificates* > *CA Certificates*.
2. Select the certificate or certificates that you would like to delete and select *Delete*.
3. Select *OK* in the confirmation dialog box to delete the certificate.

Certificate revocation lists

When you apply for a signed personal or group certificate to install on remote clients, you can obtain the corresponding root certificate and Certificate Revocation List (CRL) from the issuing CA. When you receive the signed personal or group certificate, install the signed certificate on the remote client(s) according to the browser documentation. Install the corresponding root certificate (and CRL) from the issuing CA on the FortiAnalyzer unit according to the procedures given below.

To import a CRL:

1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the *Import* button.

   The *Import* dialog box opens.
3. Select *Choose File*, browse to the location of the CRL, and select *OK*.
4. Select *Choose File*, browse to the location of the certificate, and select *OK*.

To view a CRL:

1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the CRL that you would like to see details about, then select *View Certificate Detail*.

   The *Result* page opens.
3. When you are finished viewing the CRL details, select *OK* to return to the CRL list.

To delete a CRL:

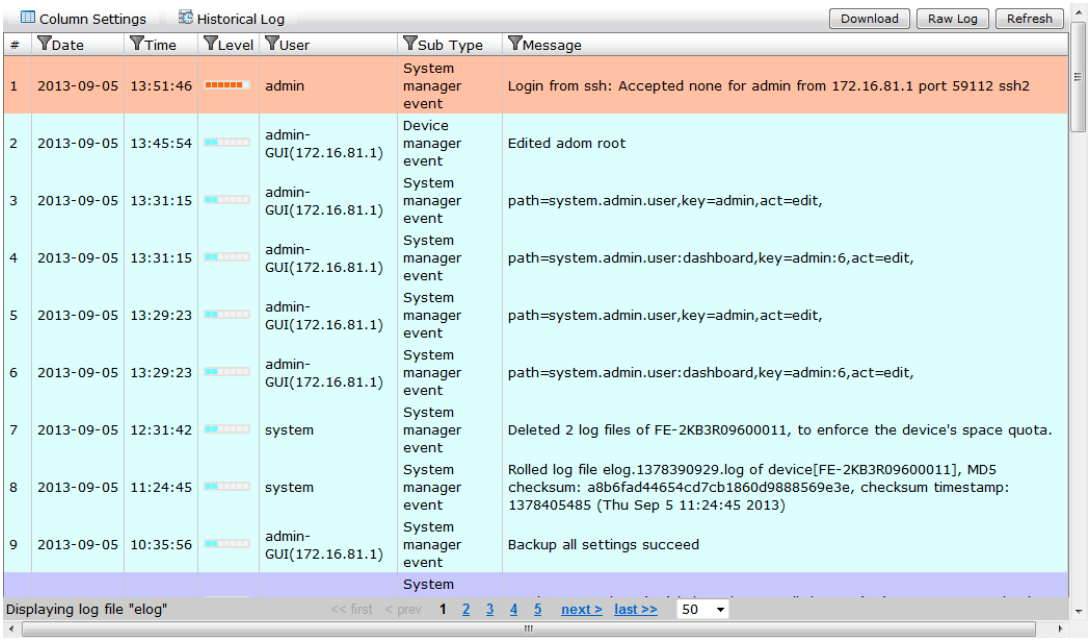
1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the CRL or CRLs that you would like to delete and select *Delete*.
3. Select *OK* in the confirmation dialog box to delete the CRL.

Event log

The logs created by Fortinet are viewable within the Web-based Manager. You can use the *FortiAnalyzer Log Message Reference*, available in the Fortinet Document Library to interpret the messages. You can view log messages in the FortiAnalyzer Web-based Manager that are stored in memory or on the internal hard disk, and use the column filters to filter the event logs that are displayed.

Go to *System Settings* > *Event Log* to view the local log list.

Figure 80: Local log list



The following information is available:

Column Settings	Select to open the column settings dialog bog. You can edit which columns are displayed and the order in which they appear.
Historical Log	Select to view the historical log.
Type	Select the type from the drop down list. Select one of the following: *Event Log, FDS Upload Log*, or *FDS Download Log*. When selecting *FDS Upload Log*, select the device from the drop-down list, and select *Go* to browse logs. When selecting *FDS Download Log*, select the service (*FDS, FCT*) from the *Service* drop-down list, select the event type (*All Event, Push Update, Poll Update, Manual Update*) from the *Event* drop-down list, and *Go* to browse logs.
Download	Select to download the event log elog. You can download the file as a comma separated value (CSV) file or in a normal format. Select *OK* to save the file to your management computer.
Raw Log/Formatted Table	Select to display either raw logs for a formatted table.

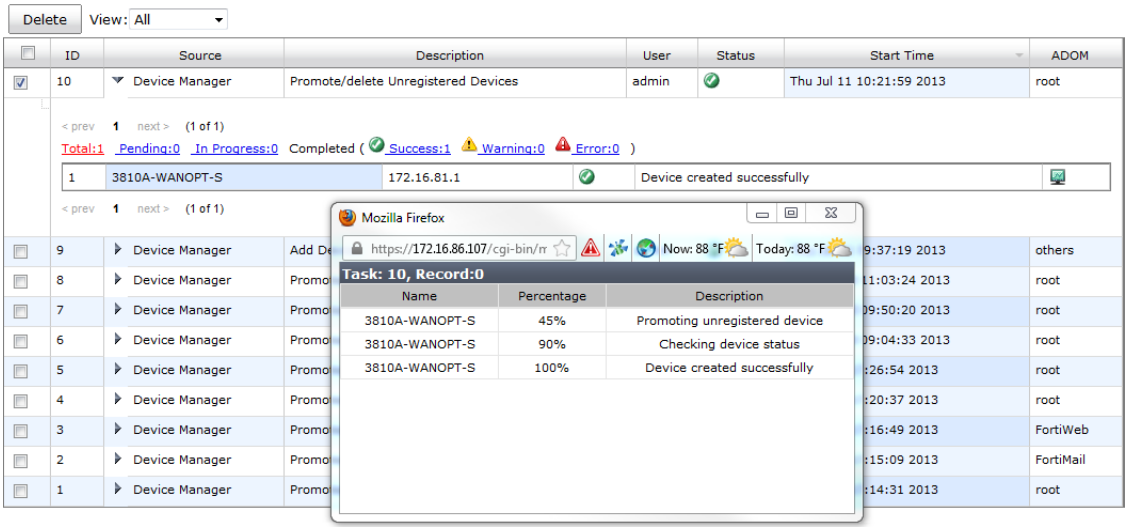
Refresh	Select to refresh the information displayed in the log table.
#	The log number.
Date	The date that the log file was generated. Select the filter icon to create a filter for this column. Select the checkbox to enable this filter and specify the from and to date in the format YYYY-MM-DD. Select *Apply* to apply the filter. You can also clear all filters.
Time	The time that the log file was generated. Select the filter icon to create a filter for this column. Select the checkbox to enable this filter and specify the from and to time in the format HH:MM:SS. Select *Apply* to apply the filter. You can also clear all filters.
Level	The log level. Select the filter icon to create a filter for this column. Select the checkbox to enable this filter. Select a value for the field from the drop-down list, select the checkbox (NOT) if required, and select the level from the drop-down list. Select *Apply* to apply the filter. You can also clear all filters.
User	User information. Select the filter icon to create a filter for this column. Select the checkbox to enable this filter. Select a value for the field from the drop-down list, select the checkbox (NOT) if required, and enter the username in the text field. Select *Apply* to apply the filter. You can also clear all filters.
Sub Type	Log sub-type information. Select the filter icon to create a filter for this column. Select the checkbox to enable this filter, then select one or more of the event types. Select *Apply* to apply the filter. You can also clear all filters. The available event types are: *System manager event*, *FG-FM protocol event*, *Device configuration event*, *Deployment manager event*, *Real-time monitor event*, *Log and report manager 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	Log message details. Select the filter icon to create a filter for this column. Select the checkbox to enable this filter. Select a value for the field from the drop-down list, select the checkbox (NOT) if required, and enter a message in the text field. Select *Apply* to apply the filter. You can also clear all filters.
Page navigation	Use these page options to browse logs. You can select to display 50, 100, or 200 logs from the drop-down list.

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 in the *View* field. Select the history icon for task details.

Figure 81: Task monitor window



The following information is available:

Delete	Remove the selected task or tasks from the list.
View	Select which tasks to view from the drop-down list, based on their status. Select one of the following: *Running, Pending, Done, Error, Cancelling, Cancelled, Aborting, Aborted, Warning*, or *All*.
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.
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 FortiAnalyzer system stopped performing this task. • *Aborting*: The FortiAnalyzer 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 associated with the task.

Advanced

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

SNMP v1/v2c	Select to configure FortiGate and FortiAnalyzer reporting through SNMP traps. See “SNMP v1/v2c” on page 113.
Mail Server	Select to configure mail server settings. See “Mail server” on page 118.
Syslog Server	Select to configure syslog server settings. See “Syslog server” on page 118.
Meta Fields	Select to configure meta-fields. See “Meta fields” on page 119.
Device Log Settings	Select to configure log settings and access and to view the task monitor. See “Device log settings” on page 121
File Management	Select to configure automatic deletion settings for file and reports. See “File management” on page 122.
Advanced settings	Select to configure ADOM mode, download the WSDL file, and configure the task list size. See “Advanced settings” on page 123.

SNMP v1/v2c

Simple Network Management Protocol (SNMP) allows you to monitor hardware on your network. You can configure the hardware, such as the FortiAnalyzer SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers. An SNMP manager, or host, is typically a computer running an application that can read the incoming trap and event messages from the agent and send out SNMP queries to the SNMP agents. A FortiManager unit can act as an SNMP manager, or host, to one or more FortiAnalyzer units.

By using an SNMP manager, you can access SNMP traps and data from any FortiAnalyzer interface configured for SNMP management access. Part of configuring an SNMP manager is to list it as a host in a community on the FortiAnalyzer unit it will be monitoring. Otherwise the SNMP monitor will not receive any traps from that FortiAnalyzer unit, or to query that unit.

You can configure the FortiAnalyzer unit to respond to traps and send alert messages to SNMP managers that were added to SNMP communities. When you are configuring SNMP, you need to first download and install both the FORTINET-CORE-MIB.mib and FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib files so that you can view these alerts in a readable format. The Fortinet MIB contains support for all Fortinet devices, and includes some generic SNMP traps; information responses and traps that FortiAnalyzer units send are a subset of the total number supported by the Fortinet proprietary MIB.

Your SNMP manager may already include standard and private MIBs in a compiled database which is all ready to use; however, you still need to download both the FORTINET-CORE-MIB.mib and FORTINET-FORTIANALYZER-MIB.mib files regardless.

FortiAnalyzer SNMP is read-only: SNMP v1 and v2 compliant SNMP managers have read-only access to FortiAnalyzer system information and can receive FortiAnalyzer traps. RFC support includes most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II). FortiAnalyzer units also use object identifiers from the Fortinet proprietary MIB.

For more information about the MIBs and traps that are available for the FortiAnalyzer unit, see "SNMP MIB Support" on page 200.

SNMP traps alert you to events that happen, such as an a log disk being full or a virus being detected.

SNMP fields contain information about your FortiAnalyzer unit, such as percent CPU usage or the number of sessions. This information is useful to monitor the condition of the unit, both on an ongoing basis and to provide more information when a trap occurs.

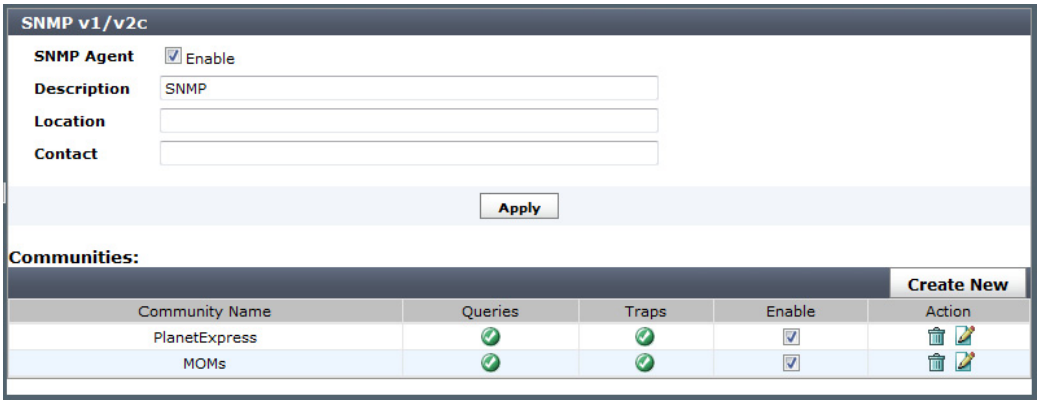
Configuring the SNMP agent

The SNMP Agent sends SNMP traps that originate on the FortiAnalyzer system to an external monitoring SNMP manager defined in one of the FortiAnalyzer 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 FortiAnalyzer system to determine if it is operating properly, or if there are any critical events occurring. The description, location, and contact information for this FortiAnalyzer 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 FortiAnalyzer system requires attention.

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

Figure 82:SNMP v1/v2c dialog box



Configure the following settings:

SNMP Agent	Select to enable the FortiAnalyzer SNMP agent. When this is enabled, it sends FortiAnalyzer SNMP traps.
Description	Enter a description of this FortiAnalyzer system to help uniquely identify this unit.
Location	Enter the location of this FortiAnalyzer system to help find it in the event it requires attention.
Contact	Enter the contact information for the person in charge of this FortiAnalyzer system.

Communities	The list of SNMP communities added to the FortiAnalyzer 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 115.
Community Name	The name of the SNMP community.
Queries	The status of SNMP queries for each SNMP community.
Traps	The status of SNMP traps for each SNMP community.
Enable	Select to enable or unselect to disable the SNMP community.
Delete icon	Select to remove an SNMP community.
Edit icon	Select to edit an SNMP community.

Configuring an SNMP community

An SNMP community is a grouping of devices for network administration purposes. Within that SNMP community, devices can communicate by sending and receiving traps and other information. One device can belong to multiple communities, such as one administrator terminal monitoring both a firewall SNMP community and a printer SNMP community.

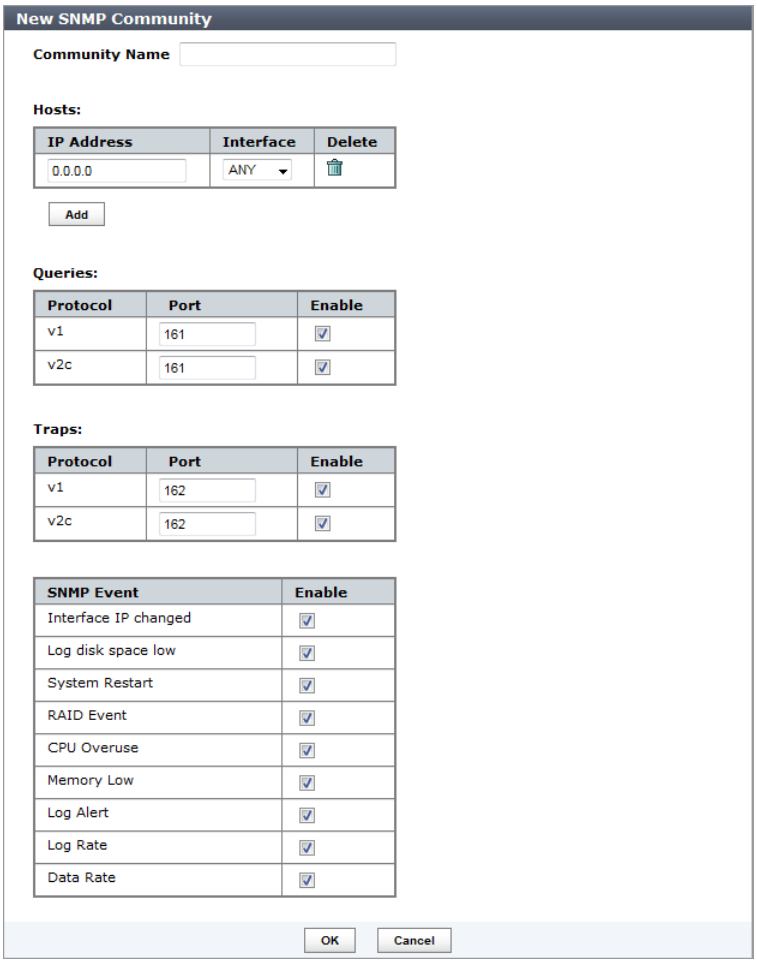
You can add an SNMP community to define a destination IP address that can be selected as the recipient (SNMP manager) of FortiAnalyzer unit SNMP alerts. Defined SNMP communities are also granted permission to request FortiAnalyzer unit system information using SNMP traps.

Each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiAnalyzer unit for a different set of events. You can also add the IP addresses of up to eight SNMP managers to each community.

To create a new SNMP community:

1. Go to *System Settings* > *Advanced* > *SNMP v1/v2c*.
2. Ensure that the *SNMP Agent* is enabled and, under *Communities*, select *Create New*.
   The *New SNMP Community* dialog box opens.

Figure 83: New SNMP community



3. Enter the following information as required.

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 FortiAnalyzer that can use the settings in this SNMP community to monitor the FortiAnalyzer 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 ( )	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 FortiAnalyzer system uses to send SNMP v1 and SNMP v2c queries to the FortiAnalyzer in this community. Enable queries for each SNMP version that the FortiAnalyzer system uses. ***Note:*** The SNMP client software and the FortiAnalyzer unit must use the same port for queries.
Traps	Enter the Remote port numbers (162 by default) that the FortiAnalyzer system uses to send SNMP v1 and SNMP v2c traps to the FortiAnalyzer in this community. Enable traps for each SNMP version that the FortiAnalyzer system uses. ***Note:*** The SNMP client software and the FortiAnalyzer unit must use the same port for traps.
SNMP Event	Enable the events that will cause the FortiAnalyzer unit to send SNMP traps to the community. SNMP events will vary based on the device model and type. These events include: • Interface IP changed • Log disk space low • System Restart • RAID Event • Power Supply Failed • CPU Overusage • Memory Low • Log Alert • Log Rate • Data Rate

4. Select *OK* to create the SNMP community.

To edit an SNMP community:

1. Go to *System Settings* > *Advanced* > *SNMP v1/v2c*.
2. In the *Action* column of the community you need to edit, select the edit icon, .
   The *Edit SNMP Community* dialog box opens.
3. Edit the SNMP community settings as required and then select *OK*.

To delete an SNMP community:

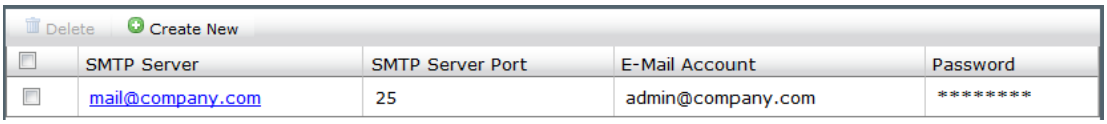
1. Go to *System Settings* > *Advanced* > *SNMP v1/v2c*.
2. In the *Action* column of the community you need to delete, select the delete icon, .
3. Select *OK* in the confirmation dialog box to delete the SNMP community.

Mail server

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

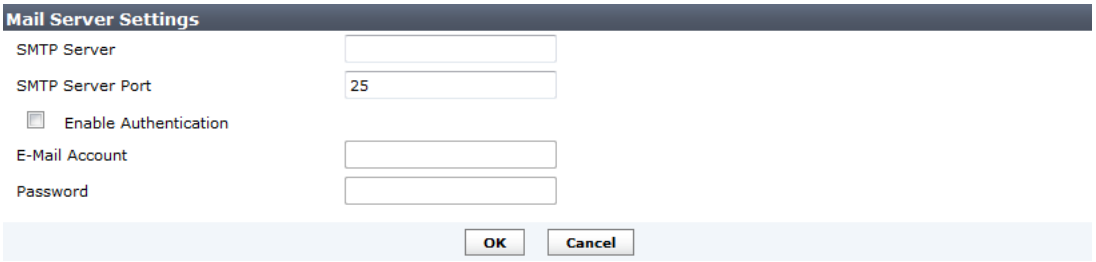
If an existing mail server is set in an *Event Handler* configuration, the delete icon is removed and the mail server entry cannot be deleted.

Figure 84: Mail server window



Select *Create New* to configure mail server settings.

Figure 85: Mail server settings



Configure the following settings and then select *OK*:

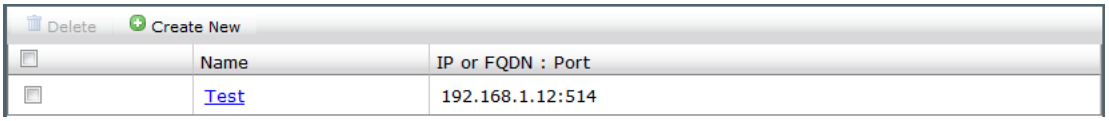
SMTP Server	Enter the SMTP server domain information, e.g. mail@company.com.
SMTP Server Port	Enter the SMTP server port number. The default port is 25.
Enable Authentication	Select to enable authentication.
Email Account	Enter an email account, e.g. admin@company.com.
Password	Enter the email account password.

Syslog server

Configure syslog server settings for alerts, edit existing settings, or delete syslog servers. Select *Create New* to add a new syslog server.

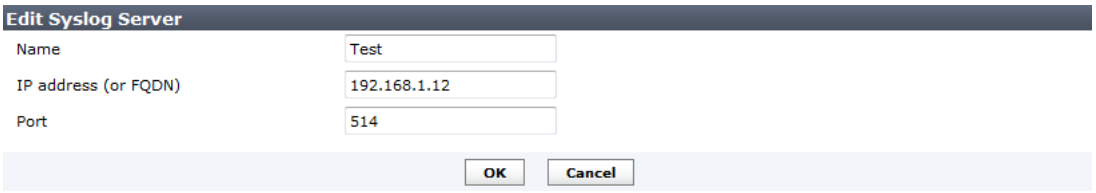
If an existing syslog server is set in an *Event Handler* configuration, the delete icon is removed and the syslog server entry cannot be deleted.

Figure 86: Syslog server window



Select *Create New* to configure a new syslog server.

Figure 87: Syslog server settings



Configure the following settings and then select *OK*:

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

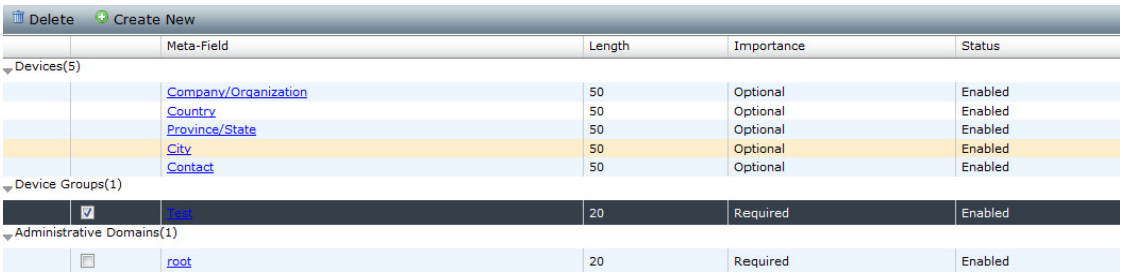
Meta fields

Metafields allow administrators to add extra information when configuring, adding, or maintaining FortiGate units. You can make the fields mandatory or optional, and set the length 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.

Go to *System Settings* > *Advanced* > *Meta Fields* to configure metafields.

Figure 88: System metadata



The following information is available:

Create New	Create a new metadata field for this object. See “To create a new metadata field:” on page 120.
Delete	Delete the selected metadata field. See “To delete metadata fields:” on page 120.

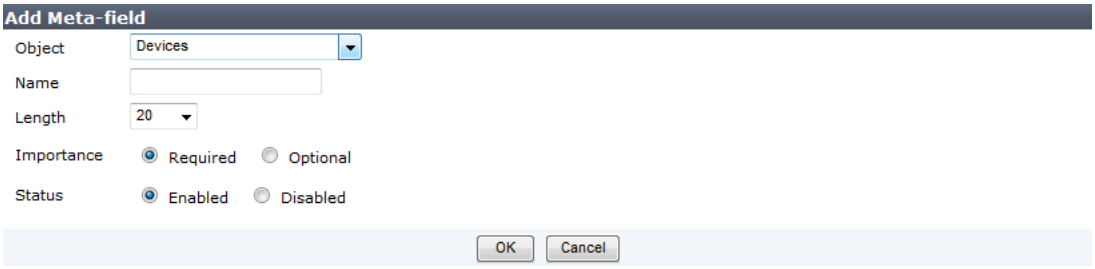
Meta-Field	The name of this metadata field. Select the name to edit this field. See "To edit a metadata field:" on page 120.
Length	The maximum length of this metadata field.
Importance	Indicates whether this field is required or optional.
Status	Indicates whether this field is enabled or disabled.

To create a new metadata field:

1. Go to *System Settings* > *Advanced* > *Meta Fields.*
2. Select *Create New*.

   The *Add Meta-field* window opens.

Figure 89: Add a meta-field



3. Configure the following settings:

Object	The system object to which this metadata field applies. Select either *Devices*, *Device Groups*, or *Administrative Domains*.
Name	Enter the label to use for the field.
Length	Select the maximum number of characters allowed for the field from the drop-down list (*20*, *50*, or *255*).
Importance	Select *Required* to make the field compulsory, otherwise select *Optional.*
Status	Select *Disabled* to disable this field. The default selection is *Enabled*.

4. Select *OK* to create 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, then select *OK* to apply the changes.

To delete metadata fields:

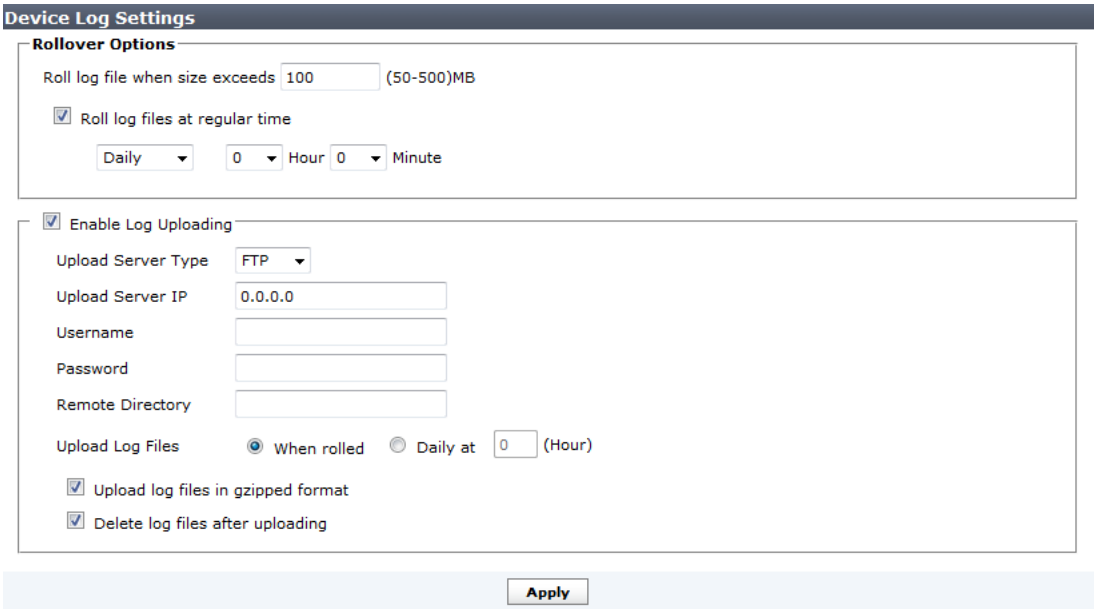
1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Select meta fields that you would like to delete. The default meta fields cannot be deleted.
3. Select *Delete*, , in the toolbar, then select *OK* in the confirmation box to delete the fields.

Device log settings

The device log settings menu allows you to configure event logging to disk and log rollover and upload options. For more information, see “Configuring rolling and uploading of logs” on page 150.

Go to *System Settings* > *Advanced* > *Device Log Settings* to configure device log settings.

Figure 90: Device log settings window



Configure the following settings and select *Apply* to apply your changes:

Rollover Options	
Roll log file when size exceeds	Enter the log file size, from 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.

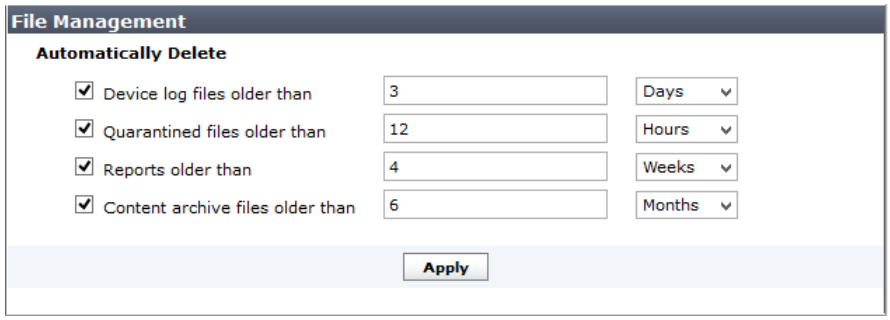
Upload Log Files	Select to upload log files when they are rolled according to settings selected under *Roll Logs* or daily at a specific hour.
Upload rolled files in gzipped format	Select to gzip the logs before uploading. This will result in smaller logs, and faster upload times.
Delete files after uploading	Select to remove device log files from the FortiAnalyzer system after they have been uploaded to the Upload Server.

File management

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

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

Figure 91: File Management

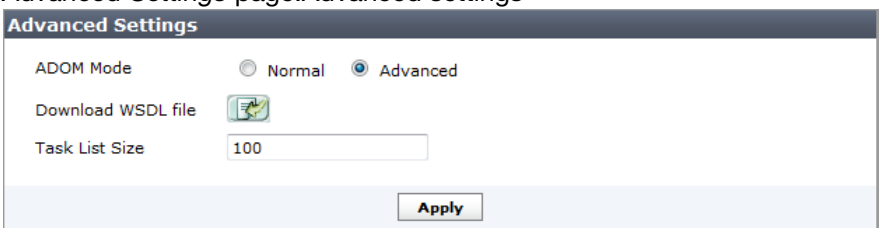


Configure the following settings:

Device log files older than	Select to enable this feature, enter a value in the text field, then select the time period from the drop-down list (*Hours*, *Days*, *Weeks*, or *Months*)
Quarantined files older than	Select to enable this feature, enter a value in the text field, and select the time period from the drop-down list.
Reports older than	Select to enable this feature, enter a value in the text field, and select the time period from the drop-down list.
Content archive files older than	Select to enable this feature, enter a value in the text field, and select the time period from the drop-down list.

Advanced settings

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



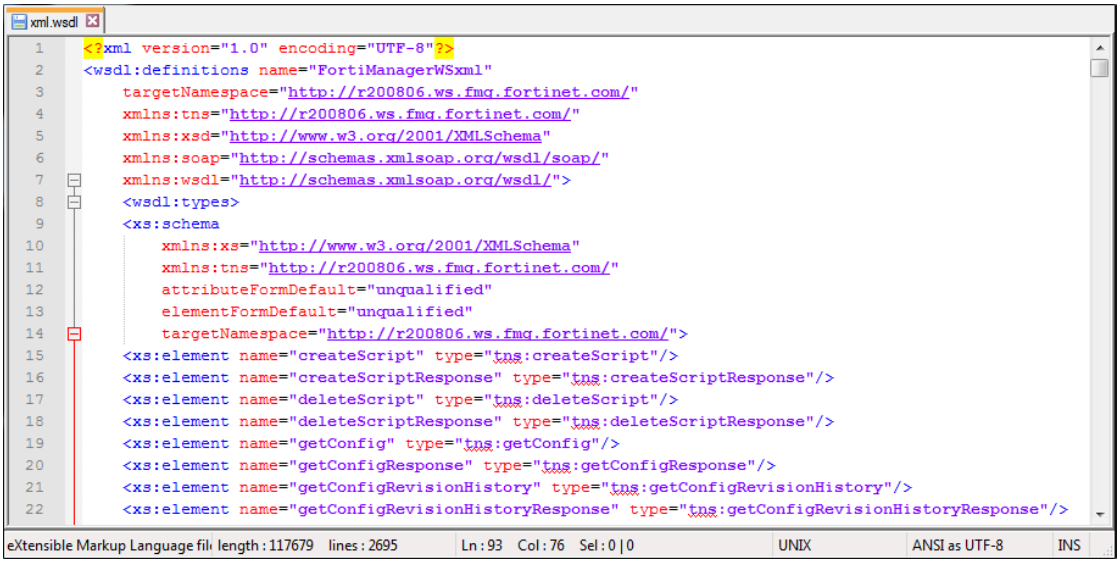
Advanced ADOM mode will allow users to assign VDOMs from a single device to different ADOMs, but will result in a reduced operation mode and more complicated management scenarios. It is recommended for advanced users only.

Configure the following settings and then select *Apply*:

ADOM Mode	Select either *Normal* or *Advanced*. In normal mode, you can only add FortiGate devices to an ADOM. In advanced mode, you can add FortiGate devices and/or their VDOMs to an ADOM.
Download WSDL file	Select to download the FortiAnalyzer unit's 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 FortiAnalyzer unit will accept, as well as the response to expect. Using the WSDL file, third-party or custom applications can communicate with the FortiAnalyzer unit and operate it or retrieve information just as an admin user would from the Web-based Manager or CLI.
Task List Size	Set a limit on the size of the task list.

Figure 92 shows an example WSDL file.

Figure 92: Example WSDL file

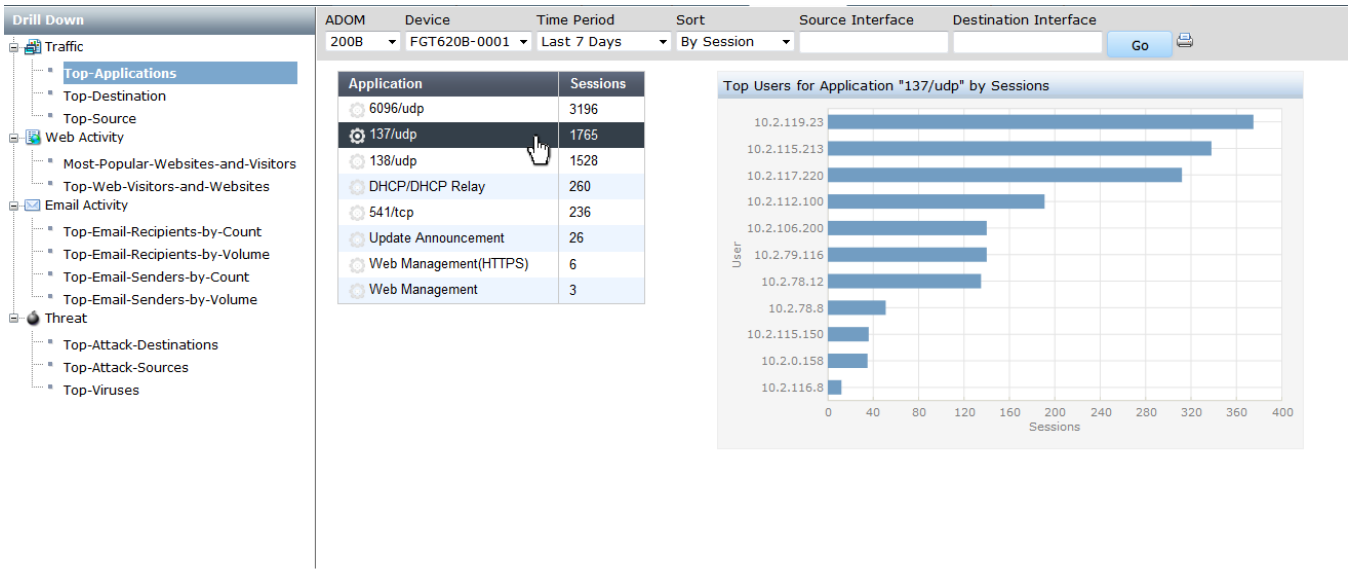


Drill Down

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.

The Drill Down tab is only available when the FortiAnalyzer unit operation mode is *Analyzer*.

Figure 93: Drill Down tab and data



Traffic

FortiAnalyzer has a fixed subset of drill downs for traffic activity. You can view and drill down top applications, destinations, and source data for individual devices, VDOMs, or log arrays that are configured to log to your FortiAnalyzer 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, enter a source 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 displayed table, 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.
3. Select the print icon,  , in the toolbar to print the drill down data.

Web activity

FortiAnalyzer 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 FortiAnalyzer 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 displayed table, 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.
3. Select the print icon,  , in the toolbar to print the drill down data.

Email activity

FortiAnalyzer 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 FortiAnalyzer device. This data can be populated for the last 30 minutes, 1 hour, 4 hours, 12 hours, 1 day or 7 days.

To display email 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 displayed table, 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.
3. Select the print icon, , in the toolbar to print the drill down data.

Threat

FortiAnalyzer 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 FortiAnalyzer device. This data can be populated for the last 30 minutes, 1 hour, 4 hours, 12 hours, 1 day or 7 days.

To display threat 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 displayed table, 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.
3. Select the print icon, , in the toolbar to print the drill down data.

Event Management

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

Events can also be monitored, and the logs associated with a given event can be viewed.

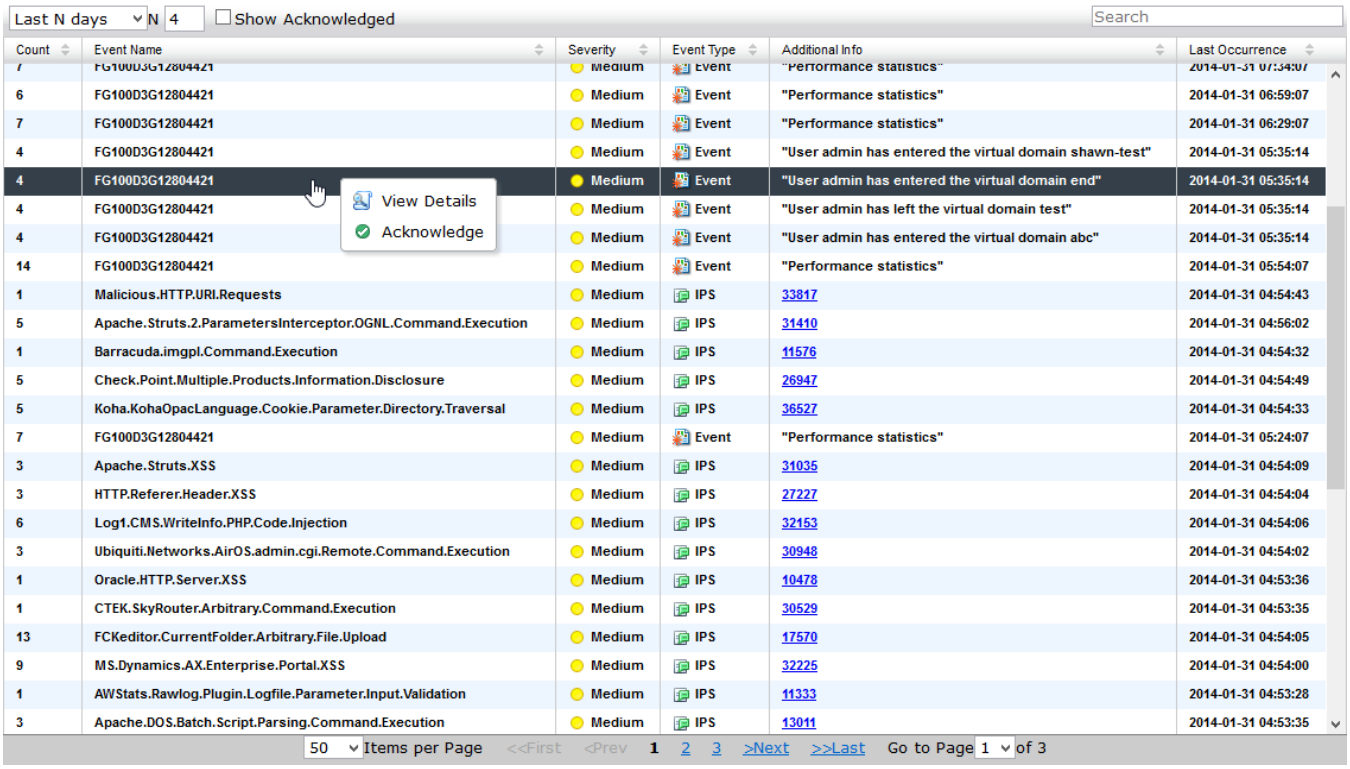
The *Event Management* tab is only available when the FortiAnalyzer unit operation mode is *Analyzer*.

Events

The events page provides a list of the generated events. Right-clicking on an event in the table gives you the option of viewing event details including the raw log entries associated with that event, adding review notes, and acknowledging the event.

To view events, go to the *Event Management* tab and select *Event Management* > *All Events.* You can also view events by severity and by handler. When ADOMs are enabled, select the ADOM, and then select *All Events*.

Figure 94: Events page



Count	Event Name	Severity	Event Type	Additional Info	Last Occurrence
6	FG100D3G12804421	Medium	Event	"Performance statistics"	2014-01-31 06:59:07
7	FG100D3G12804421	Medium	Event	"Performance statistics"	2014-01-31 06:29:07
4	FG100D3G12804421	Medium	Event	"User admin has entered the virtual domain shawn-test"	2014-01-31 05:35:14
4	FG100D3G12804421	Medium	Event	"User admin has entered the virtual domain end"	2014-01-31 05:35:14
4	FG100D3G12804421	Medium	Event	"User admin has left the virtual domain test"	2014-01-31 05:35:14
4	FG100D3G12804421	Medium	Event	"User admin has entered the virtual domain abc"	2014-01-31 05:35:14
14	FG100D3G12804421	Medium	Event	"Performance statistics"	2014-01-31 05:54:07
1	Malicious.HTTP.URI.Requests	Medium	IPS	33817	2014-01-31 04:54:43
5	Apache.Struts.2.ParametersInterceptor.OGNL.Command.Execution	Medium	IPS	31410	2014-01-31 04:56:02
1	Barracuda.imgpl.Command.Execution	Medium	IPS	11576	2014-01-31 04:54:32
5	Check.Point.Multiple.Products.Information.Disclosure	Medium	IPS	26947	2014-01-31 04:54:49
5	Koha.KohaOpacLanguage.Cookie.Parameter.Directory.Traversal	Medium	IPS	36527	2014-01-31 04:54:33
7	FG100D3G12804421	Medium	Event	"Performance statistics"	2014-01-31 05:24:07
3	Apache.Struts.XSS	Medium	IPS	31035	2014-01-31 04:54:09
3	HTTP.Referer.Header.XSS	Medium	IPS	27227	2014-01-31 04:54:04
6	Log1.CMS.WriteInfo.PHP.Code.Injection	Medium	IPS	32153	2014-01-31 04:54:06
3	Ubiquiti.Networks.AirOS.admin.cgi.Remote.Command.Execution	Medium	IPS	30948	2014-01-31 04:54:02
1	Oracle.HTTP.Server.XSS	Medium	IPS	10478	2014-01-31 04:53:36
1	CTEK.SkyRouter.Arbitrary.Command.Execution	Medium	IPS	30529	2014-01-31 04:53:35
13	FCKeditor.CurrentFolder.Arbitrary.File.Upload	Medium	IPS	17570	2014-01-31 04:54:05
9	MS.Dynamics.AX.Enterprise.Portal.XSS	Medium	IPS	32225	2014-01-31 04:54:00
1	AWStats.Rawlog.Plugin.Logfile.Parameter.Input.Validation	Medium	IPS	11333	2014-01-31 04:53:28
3	Apache.DOS.Batch.Script.Parsing.Command.Execution	Medium	IPS	13011	2014-01-31 04:53:35

The following information and options are available:

Time Period	Select a time period from the drop-down list. Select one of: *Last 30 mins*, *Last 1 hour*, *Last 4 hours*, *Last 12 hours*, *Last 1 day*, *Last 7 days*, *Last N hours*, *Last N days*, *All*. If applicable, enter the number of days or hours for N in the *N* text box.
Show/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 Name	The name of the event. Click the heading to sort events by event name.
Severity	The severity level of the event. Event severity level is a user configured variable. The severity can be *Critical*, *High*, *Medium*, or *Low*. Click the heading to sort events by severity.
Event Type	The event type. For example, *Traffic* or *Event.* Click the heading to sort events by event type.
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.
Page navigation	Adjust the number of logs that are listed per page and browse through the pages.

Right-click on an event in the list to open the right-click menu. The following options are available:

View Details	The *Event Details* page is displayed. See “Event details” on page 129.
Acknowledge	Acknowledge an event. If *Show Acknowledge* is not selected, the event will be hidden. See “Acknowledge events” on page 130.

Event details

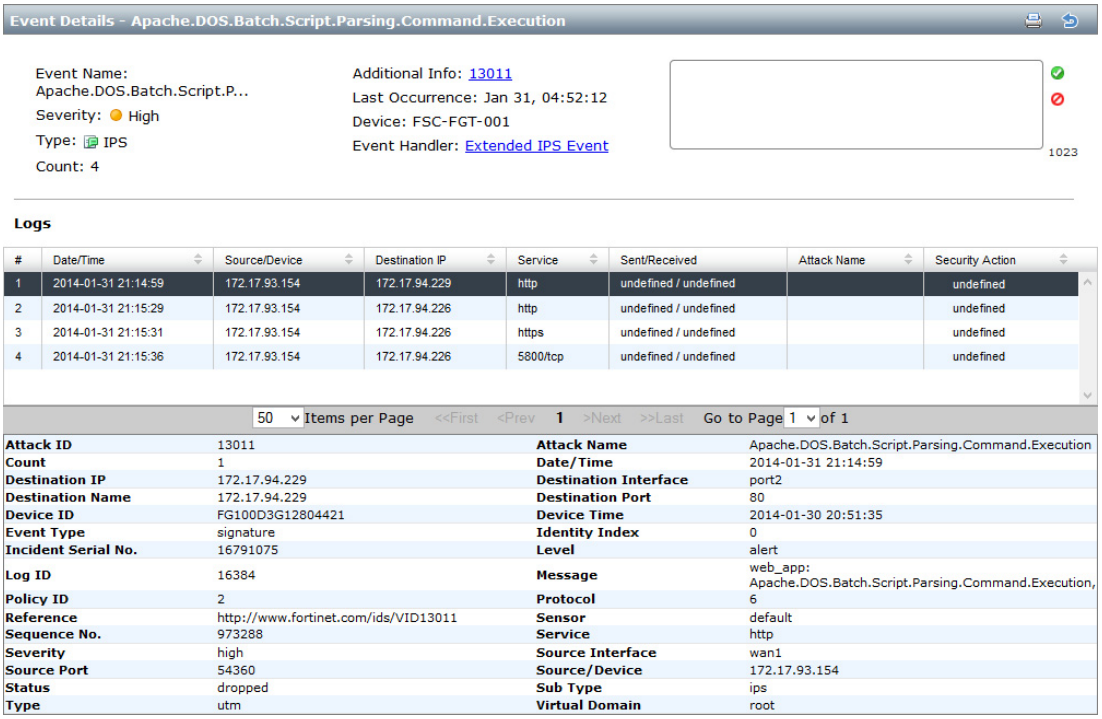
Event details provides a summary of the event including the event name, severity, type, count, additional information, last occurrence, device, event handler, raw log entries, and review notes. You can also acknowledge and print events in this page.

To view log messages associated with an event:

1. In the events list, either double-click on an event or right-click on an event then select *View Details* in the right-click menu.

   The *Event Details* page opens.

   Figure 95: Event details page



2. The following options and information are available:

Print	Select the print icon, , to print the event details page. The log details pane is not printed.
Return	Select the return icon, , to return to the *All Events* page.
Event Name	The name of the event, also displayed in the title bar.
Severity	The severity level configured for the event handler.
Type	The event category of the event handler.
Count	The number of logged events associated with the event.
Additional Info	This field either displays additional information for the event or a link to the FortiGuard Encyclopedia. A link will be displayed for AntiVirus, Application Control, and IPS event types.
Last Occurrence	The date and time of the last occurrence.

Device	The device hostname associated with the event.
Event Handler	The name of the event handler associated with the event. Select the link to edit the event handler. See “Event handler” on page 131.
Text box	Optionally, you can enter a 1023 character comment in the text field. Select the save icon, , to save the comment, or cancel, , to cancel your changes.
Logs	The logs associated with the log event are displayed. The columns and log fields are dependent on the event type.
Page navigation	Adjust the number of logs that are listed per page and browse through the pages.
Log details	Log details are shown in the lower content pane for the selected log. The details will vary based on the log type.

3. Select the return icon, , to return to the *All Events* page.

Acknowledge events

You can select to acknowledge events to remove them from the event list. An option has been added to this page to allow you to show or hide these acknowledged events.

To acknowledge events:

1. *From the event list, s*elect the event or events that you would like to acknowledge.
2. Right-click and select *Acknowledge* in the right-click menu.

   Select the *Show Acknowledge* checkbox in the toolbar to view acknowledged events.

Event handler

The event handler allows you to view, create new, edit, delete, clone, and search event handlers. You can select these options in the toolbar. The right-click menu includes these options and also includes the ability to enable or disable configured event handlers. You can create event handlers for a specific device, multiple devices, or log arrays. You can select to create event handlers for traffic logs or event logs.

FortiAnalyzer v5.0 Patch Release 5 or later 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.

Table 5: Default event handlers

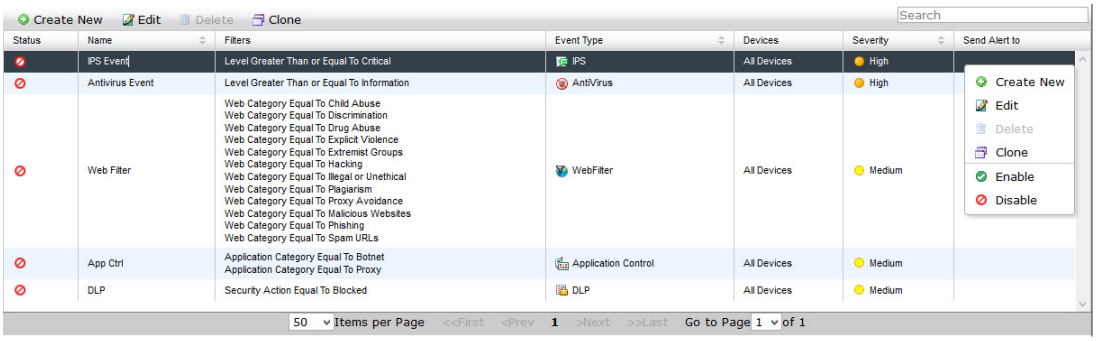
Event Handler	Description
Antivirus Event	Status: Disabled (Default) Devices: All FortiGates, All FortiCarriers (Default) Severity: High Log Type: Traffic Log Event Category: AntiVirus Group by: Virus Name Log messages that match all conditions: • *Level Greater Than or Equal To Information* Event Handling: Generate alert when at least 1 matches occurred over a period of 30 minutes. Select one of the following: *Send Alert Email*, *Send SNMP Trap to*, *Send Alert to Syslog Server*.
APP Ctrl	Status: Disabled (Default) Devices: All FortiGates, All FortiCarriers (Default) Severity: Medium Log Type: Traffic Log Event Category: Application Control Group by: Application Name Log messages that match any of the following conditions: • *Application Category Equal To Botnet* • *Application Category Equal To Proxy* Event Handling: Generate alert when at least 1 matches occurred over a period of 30 minutes. Select one of the following: *Send Alert Email*, *Send SNMP Trap to*, *Send Alert to Syslog Server*.

Table 5: Default event handlers (continued)

Event Handler	Description
DLP	Status: Disabled (Default) Devices: All FortiGates, All FortiCarriers (Default) Severity: Medium Log Type: Traffic Log Event Category: DLP Group by: DLP Rule Name Log messages that match all conditions: • *Security Action Equal To Blocked* Event Handling: Generate alert when at least 1 matches occurred over a period of 30 minutes. Select one of the following: *Send Alert Email*, *Send SNMP Trap to*, *Send Alert to Syslog Server*.
IPS Event	Status: Disabled (Default) Devices: All FortiGates, All FortiCarriers (Default) Severity: High Log Type: Traffic Log Event Category: IPS Group by: Attack Name Log messages that match all conditions: • *Level Greater Than or Equal To Critical* Event Handling: Generate alert when at least 1 matches occurred over a period of 30 minutes. Select one of the following: *Send Alert Email*, *Send SNMP Trap to*, *Send Alert to Syslog Server*.
Web Filter	Status: Disabled (Default) Devices: All FortiGates, All FortiCarriers (Default) Severity: Medium Log Type: Traffic Log Event Category: WebFilter Group by: Hostname URL Log messages that match any of the following conditions: • *Web Category Equal To Child Abuse, Discrimination, Drug Abuse, Explicit Violence, Extremist Groups, Hacking, Illegal or Unethical, Plagiarism, Proxy Avoidance, Malicious Websites, Phishing, Spam URLs* Event Handling: Generate alert when at least 1 matches occurred over a period of 30 minutes. Select one of the following: *Send Alert Email*, *Send SNMP Trap to*, *Send Alert to Syslog Server*.

Go to the *Event Management* tab and select *Event Handler* in the tree menu.

Figure 96: Event handler page



The following information and options are available:

Create New	Select to create a new event handler. This option is available in the toolbar and right-click menu. See "To create a new event handler:" on page 134.
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. See "To edit an event handler:" on page 136.
Delete	Select one or all event handlers and select delete to remove the entry or entries. This option is available in the toolbar and right-click menu. The default event handlers cannot be deleted. See "To delete an event handler:" on page 136.
Clone	Select an event handler in this page and click to clone the entry. A cloned entry will have *Copy* added to its name field. You can rename the cloned entry while editing the event handler. This option is available in the toolbar and right-click menu. See "To clone an event handler:" on page 136.
Status	The status of the event handler. This field will display when enabled and when disabled.
Name	The name of the event handler.
Filters	The filters that you have configured for the event handler.
Event Type	The event category of the event handler. One of the following: AntiVirus, Application Control, DLP, IPS, or WebFilter.
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.

Enable	Right-click an event handler and select *Enable* in the pop-up menu. See "To enable an event handler:" on page 136.
Disable	Right-click an event handler and select *Disable* in the pop-up menu. See "To disable an event handler:" on page 136.

Manage event handlers

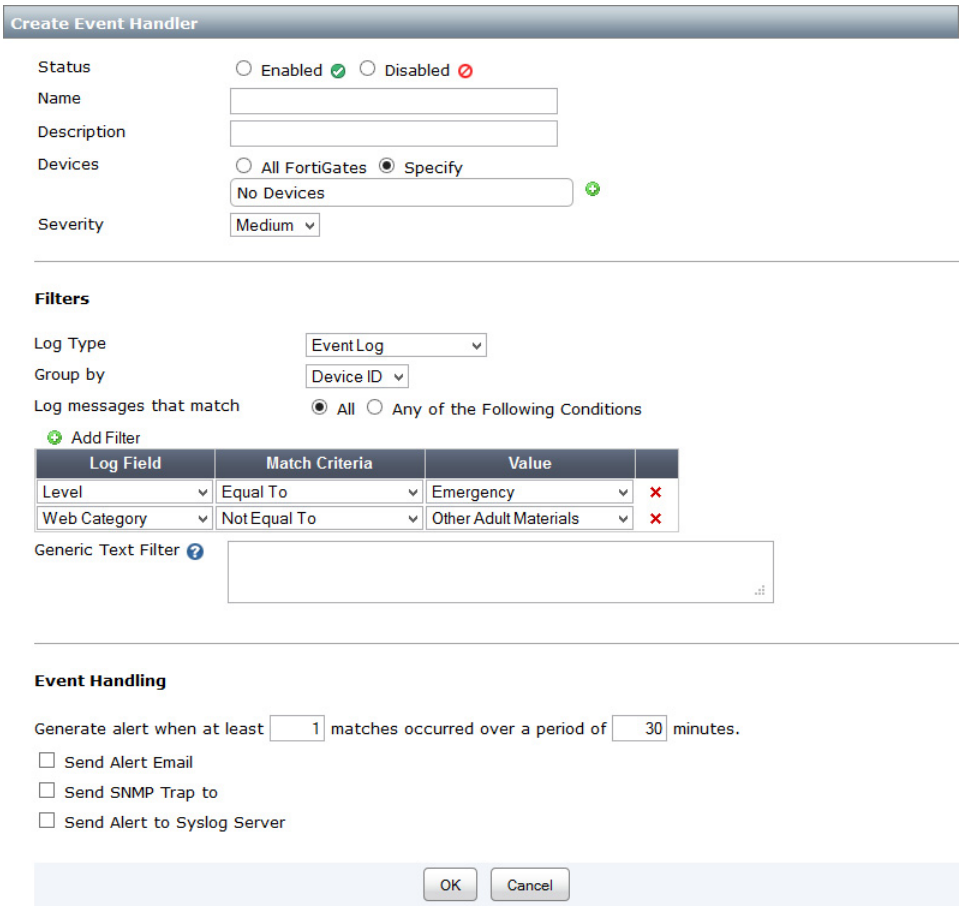
You can create traffic, event, and extended log handlers to monitor network traffic and events based on specific log filters. These log handlers can then be edited, deleted, cloned, and enabled or disabled as needed.

To create a new event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select *Create New* in the toolbar, or right-click on an the entry and select *Create New* in the right-click menu.

   The *Create Event Handler* page opens.

Figure 97: Create new event handler page



3. Configure the following settings:

Status	Enable or disable the event handler.
Name	Enter a name for the event handler.

Description	Enter a description for the event handler.
Devices	Select *All FortiGates* or select *Specify* and use the plus icon,  , 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 the log type from the drop-down list. The available options are: *Traffic Log*, *Event Log*, *Application Control*, *DLP*, *IPS*, *Virus*, and *Web Filter*.
Event Category	Select the category of event that this handler will monitor from the drop-down list. This option is only available when *Log Type* is set to *Traffic Log*.
Group by	Select the criterium by which the information will be grouped. This option is not available when *Log Type* is set to *Traffic Log*.
Log message that match	Select either *All* or *Any of the Following Conditions*.
Add Filter	Select the plus (+) symbol to add log filters.
Log Field	Select a log field to filter from the drop-down list. The available options will vary depending on the selected log type.
Match Criteria	Select a match criteria from the drop-down list. The available options will vary depending on the selected log field.
Value	Either select a value from the drop-down list, or enter a value in the text box. The available options will vary depending on the selected log field.
Delete	Select the delete icon,  , to delete the filter. A minimum of one filter is required.
Generic Text Filter	Enter a generic text filter. For more information on creating a text filter, hover the cursor over the help icon,  .
Event Handling	
Generate alerts when at least	Enter threshold values to generate alerts. Enter the number, in the first text box, of each type of event that can occur in the number of minutes entered in the second text box.
Send Alert Email	Select the checkbox to enable. Enter an email address in the *To* and *From* text fields, enter a subject in the *Subject* field, and select the email server from the drop-down list. For information on creating a new mail server, see "Mail server" on page 118.

Send SNMP Trap to	Select the checkbox to enable this feature. Select an SNMP community from the drop-down list. For information on creating a new SNMP community, see "To create a new SNMP community:" on page 116.
Send Alert to Syslog Server	Select the checkbox to enable this feature. Select a syslog server from the drop-down list. For information on creating a new syslog server, see "Syslog server" on page 118.

4. Select *OK* to create the new event handler.

To edit an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry and either select *Edit* in the toolbar, or right-click on the entry and select *Edit* in the pop-up menu. The *Edit Event Handler* page opens.
3. Edit the settings as required.
4. Select *OK* to save the configuration.

To clone an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry and either select *Clone* in the toolbar, or right-click on the entry and select *Clone* in the pop-up menu. The *Clone Event Handler* window opens.
3. Edit the settings as required.
4. Select *OK* to save the configuration.

To delete an event handler:

1. Go to *Event Management* > *Event Handler*.
2. Select an event handler entry and either select *Delete* in the toolbar, or right-click on the entry and select *Delete* in the pop-up menu.
3. Select *OK* in the confirmation dialog box to delete the event handler.

The default event handlers cannot be deleted. Use the right-click menu to enable or disable these event handlers.

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.

Log View

Logging and reporting can help you determine what is happening on your network, as well as informing you of certain network activity, such as the detection of a virus, or IPsec VPN tunnel errors. Logging and reporting go hand in hand, and can become a valuable tool for information gathering, as well as displaying the activity that is happening on the network.

Your FortiAnalyzer device collects logs from managed FortiGate, FortiCarrier, FortiMail, and 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, or admin login or HA events occur. Event logs are important because they record Fortinet device system activity, which provides valuable information about how your Fortinet unit is performing. The FortiGate event logs includes *System*, *Router*, *VPN*, and *User* menu objects to provide you with more granularity when viewing and searching log data.

Security logs (FortiGate) record all antivirus, web filtering, application control, intrusion prevention, email filtering, data leak prevention, and VoIP activity on your managed devices.

The logs displayed on your FortiAnalyzer 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.

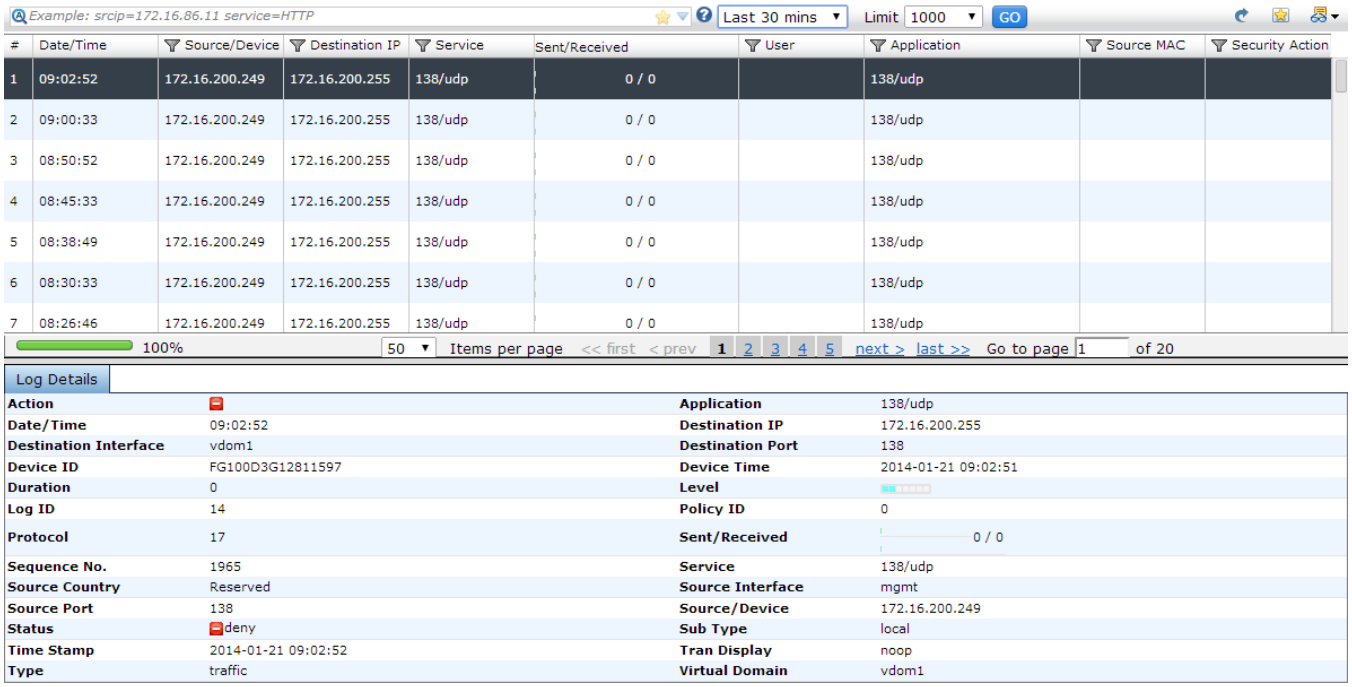
For more information on logging see the *Logging and Reporting for FortiOS v5.0 Handbook* in the Fortinet Document Library.

The *Log View* tab shows log messages for connected devices, organized by ADOMs. You can also view, import, and export log files that are 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* in the Fortinet Document Library. For more information on FortiMail raw logs, see the *FortiMail Log Message Reference*.

Figure 98: Log view



This page displays the following:

Search	Enter a search term to search the log messages. See "To perform a text search:" on page 142.
Bookmark	Select the favorites icon, , to save, or bookmark, the search term. See "Bookmarks" on page 143.
History	Select the history icon, , to repeat previous searches, select favorite searches, or quickly add filters to your search. The filters available will vary based on device and log type.
Question Mark	Hover your mouse over the help icon, , for example search syntax. See "Examples" on page 144.
Timeframe	Select a timeframe from the drop-down list. Options include: *Last 30 mins*, *Last 1 hour*, *Last 4 hours*, *Last 12 hours*, *Last 1 day*, *Last 7 days*, *Last N hours*, *Last N days*, or *Custom*. See "To customize the timeframe:" on page 142.
Limit	Select the maximum number of log entries to be displayed from the drop-down list. Options include: *1000*, *5000*, *10000*, *50000*, or *All*.

GO	Select to apply the time frame and limit to the displayed log entries. A progress bar is displayed in the lower toolbar.
Refresh	Select to refresh the log view. This option is only available when viewing historical logs.
Bookmarks	Select the bookmarks icon, , to open the *Bookmarks* dialog box and view all saved searches. See "Bookmarks" on page 143.
Pause/Resume	Select to pause, , or resume, , real time log data updates. This option is only available when viewing real time logs.
View	The view icon, , provides options for changing the manner in which the logs are displayed, and search and column options. It also provides an option for downloading logs, see "Download log messages" on page 144.
Logs	The columns and information shown in the log message list will vary depending on the selected log type, the device type, and the view settings.
Page navigation	Adjust the number of logs that are listed per page and browse through the pages.
Log Details	Detailed information on the log message selected in the log message list. The item is not available when viewing raw logs. See "Log details" on page 145 for more information.
Archive	Information about archived logs, when they are available. The item is not available when viewing raw logs, or when the selected log message has no archived logs. See "Archive" on page 145 for more information.

Customizing the log view

The log message list can show raw or formatted, real time or historical logs. The columns in the log message list can be customized to show only relevant information in your preferred order.

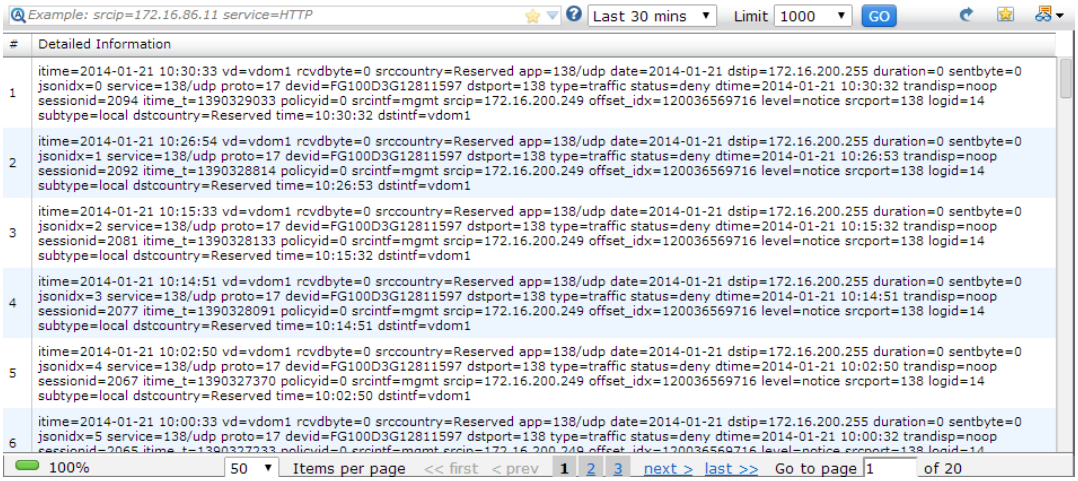
Log display

By default, historical formatted logs are shown in the log message list. You can change the view to show raw logs and both raw and formatted real time logs.

To view real time logs, in the log message list, select *View*, , then select *Realtime Log* from the drop-down menu. To return to the historical log view, select *View*, then select *Historical Log* from the drop-down menu.

To view raw logs, in the log message list, select *View*, then select *Display Raw* from the drop-down menu, Figure 99. To return to the formatted log view, select *View*, then select *Display Formatted* from the drop-down menu.

Figure 99: Raw logs



The selected log view will affect the other options that are available in the *View* drop-down menu. Real time logs cannot be downloaded, and raw logs to not have the option to customize the columns.

Columns

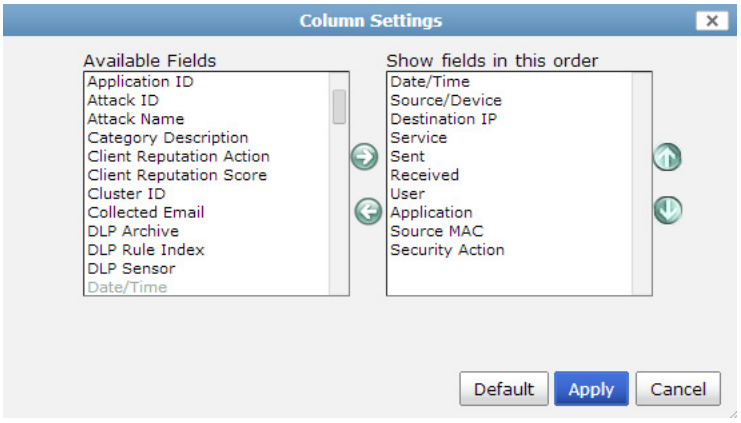
The columns displayed in the log message list can be customized and reordered as needed. Filters can also be applied to the data in a column.

To customize the displayed columns:

1. In the log message list, select *View*, then select *Column Settings* from the drop-down menu.

   The *Column Settings* dialog box opens.

   Figure 100: Column settings



2. Select which columns to hide or display:
   - To add a column to the page, in the *Available Fields* area, select the columns you want to display, then select the right arrow to move them to the *Show fields in this order* area.
   - To remove a column from the page, in the *Show fields in this order* area, select the columns you want to hide, then select the left arrow to move them to the *Available Fields* area.
   - To return all columns to their default view, select *Default*.

The available column settings will vary based on the device and log type selected.

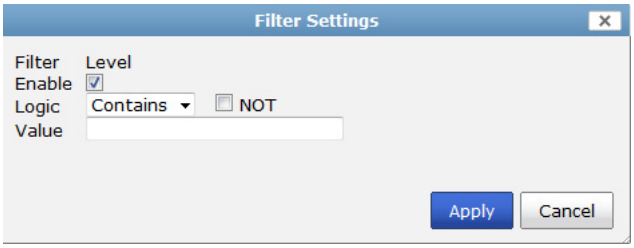
3. Adjust the order of the displayed columns:
   a. In the *Show fields in this order* area, select a column name.
   b. Select the up or down arrow to move the column up or down (left or right, respectively, in the log message list).
4. Select *Apply* to apply your changes.

To filter column data:

1. In the log message list, select *View*, then select *Enable Column Filter* from the drop-down menu to enable column filters.
2. In the heading of the column you need to filter, select the filter icon, . The filter icon will only be shown on columns that can filtered.

   The *Filter Settings* dialog box opens.

   Figure 101: Filter settings



3. Enable the filter, then enter the required information to filter the selected column.

   The filter settings will vary based on the column settings.
4. Select *Apply* to apply the filter to the data.

   The column's filter icon will turn green when the filter is enabled, . Downloading the current view will only download the log messages that meet the current filter criteria.

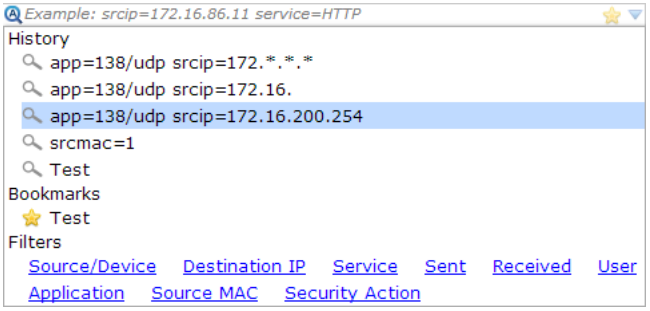
Searching log messages

Log messages can be searched based on a text string and/or timeframe. Recent searches can be quickly repeated, search terms can be saved as favorites, a timeframe can be specified or customized, and the number of displayed logs can be limited. A text string search can be case sensitive or not as required.

To perform a text search:

1. In the log message list, select *View*, then either select or deselect *Case Sensitive Search* from the drop-down menu to enable or disable case sensitivity in the search string.
2. In the log message list, enter a text string in the search field in the following ways:
   - Manually type in the text that you are searching for. Wildcard characters are accepted.
   - Right-click on the element in the list that you would like to add to the search and select *Add to search* from the pop-up menu.
   - Select a previous search, saved (bookmarked) search, or default filter, using the history icon, . The available filters will vary depending on the selected log type.

     Figure 102: Search history

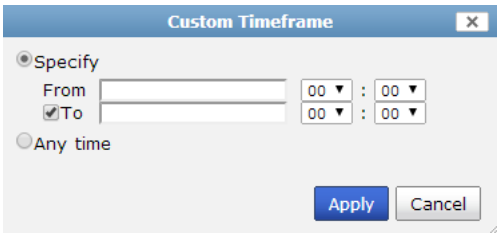
   - Paste a saved, or bookmarked, search into the search field. See “Bookmarks” on page 143.
3. Select *GO* to search the log message list.

To customize the timeframe:

1. In the log message list, open the timeframe drop-down menu, and select *Custom...*.

   The *Column Timeframe* dialog box opens.

   Figure 103: Custom timeframe

2. Specify the desired timeframe using the *From* and *To* fields, or select *Any Time* to remove any timeframe from the displayed data.
3. Select *Apply* to create the custom timeframe.

   A calendar icon, , will be shown next to the timeframe drop-down list. Select it to adjust the custom timeframe settings.
4. Select *GO* to apply your settings to the log message list.

Bookmarks

Frequently used search strings can be saved and reused as needed.

To save a search string:

1. In the log message list, after entering a search term, select the favorites icon, .
2. In the *Add to Favorites* pop-up box, enter a name for the search and adjust the search string text as needed.
3. Select *OK* to save the search as a favorite or bookmark.

   The search will now be available from the search history.

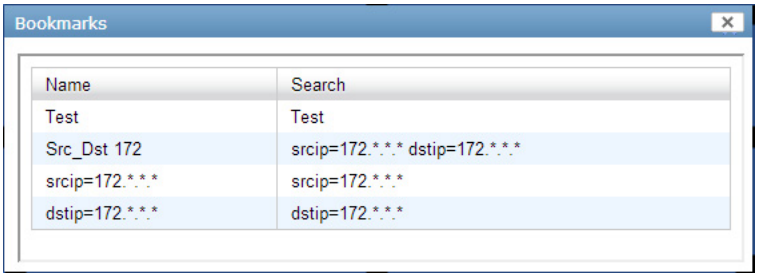
To use a saved search:

To reuse a saved search, either use the search history to select the search from the history list (see Figure 102 on page 142), or do one of the following:

1. In the log message list, select the bookmarks icon, .

   The *Bookmarks* dialog box opens.

   Figure 104: Bookmarks



2. Right-click on the search you would like to use, then select *Paste* in the pop-up menu.

   The saved search string will populate the search field.
3. Select *GO* to search the log message.

To delete a saved search string:

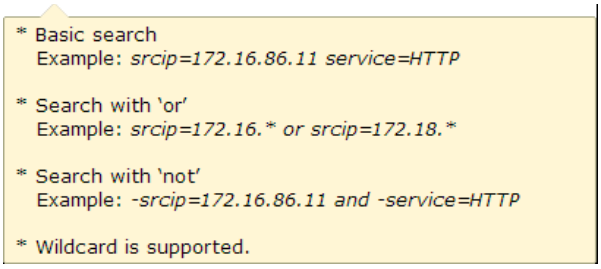
1. In the log message list, select the bookmarks icon, .

   The *Bookmarks* dialog box opens.
2. Right-click on the search you would like to delete, then select *Delete* in the pop-up menu.
3. Select *OK* in the confirmation dialog box to delete the saved search.

Examples

To view example text search strings, hover your cursor over the help icon, .

Figure 105: Example searches



- The first example will search for log messages with a source IP of 172.16.86.11 and a service of HTTP. Because it is not specified, the and operator is assumed, meaning that both conditions must be met for the log message to be included in the search results.
- The second example will search for any log messages with source IP addresses that start with either 172.16 or 172.18. Notice the use of the * wildcard. The use of the *or* operator means that either condition can be met for the log message to be included in the search results.
- The third example will search for any log message that do not have a source IP address of 172.16.86.11 and a service of HTTP. The use of the *and* operator means that both conditions must be met for the log message to be excluded from the search results.

Download log messages

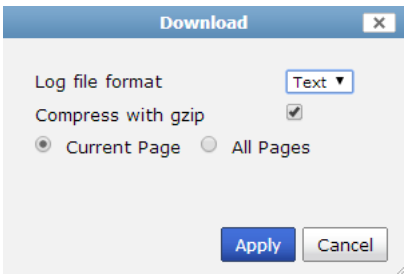
Log messages can be downloaded to the management computer as a text or CSV file. Real time logs cannot be downloaded.

To download log messages:

1. In the log message list, select *View*, then select *Download*.

   The *Download* dialog box opens.

   Figure 106: Download log messages

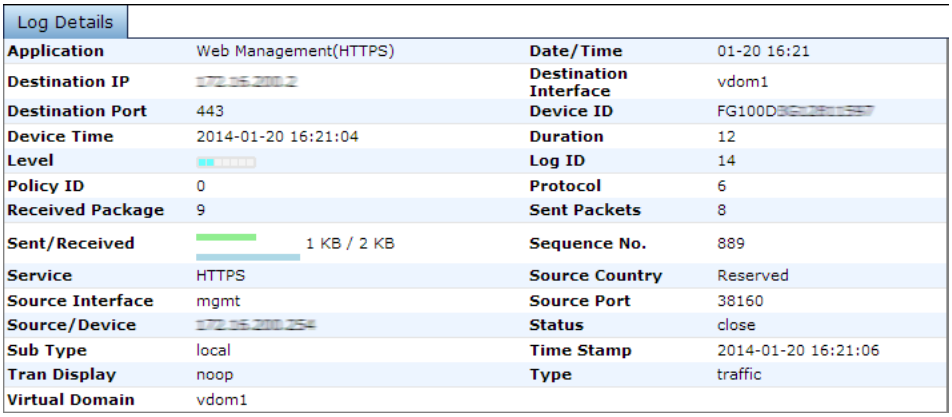
2. Select a log format from the drop down list, either *Text* or *CSV*.
3. Select *Compress with gzip* to compress the downloaded file.
4. Select *Current Page* to download only the current log message page, or *All Pages* to download all of the pages in the log message list.
5. Select *Apply* to download the log messages to the management computer.

Log details

Log details can be viewed for any of the collected logs. The details provided in vary depending on the device and type of log selected. The fields available in the this pane cannot be edited or re-organized.

To view log details, select the log in the log message list. The log details frame will be displayed in the lower frame of the content pane. Log details are not available when viewing raw logs.

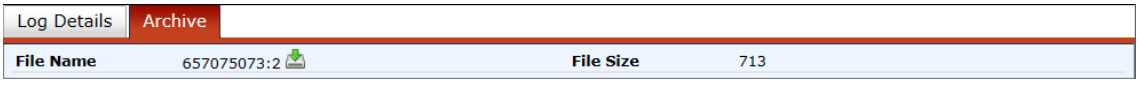
Figure 107: Log details



Archive

The *Archive* tab is displayed next to the *Log Details* tab in the lower content pane when archived logs are available.

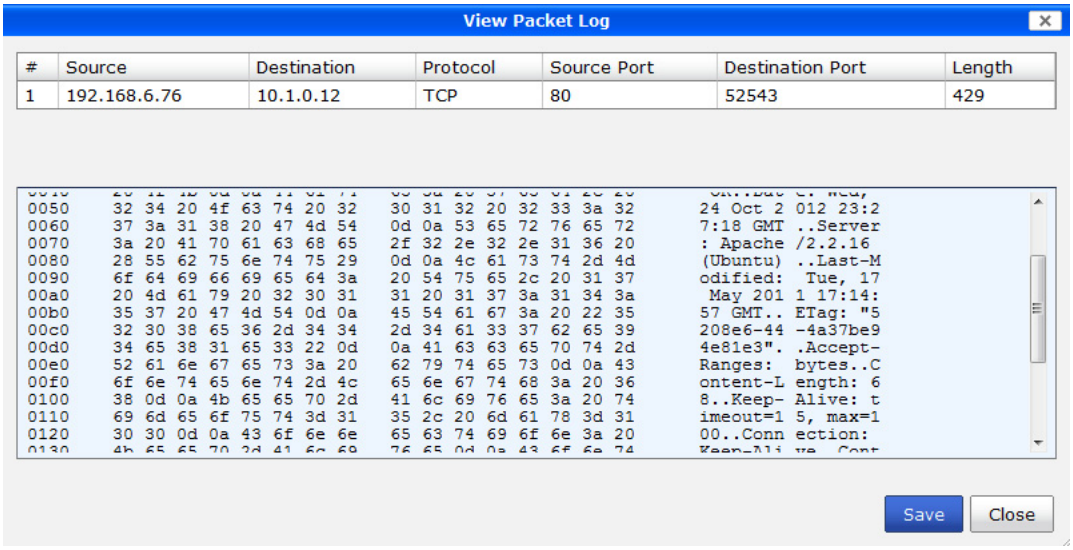
Figure 108: Log archive



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 109: View packet log



Browsing log files

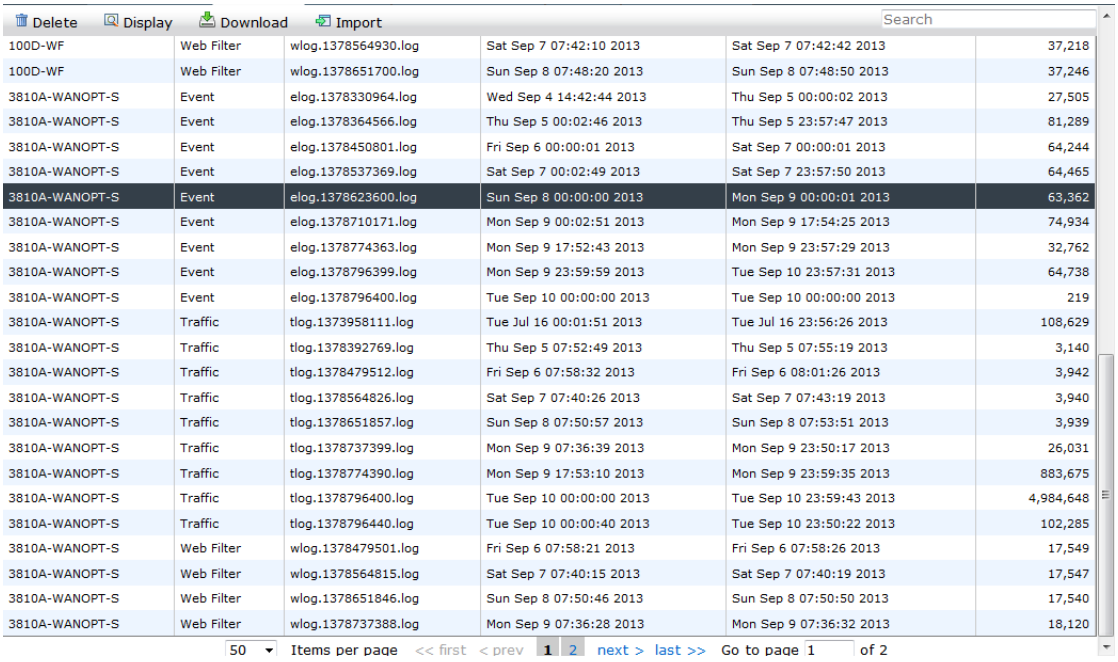
Go to *Log View* > *Log Browse* to view log files stored for devices. On this page you can display, download, delete, and import log files.

When a log file reaches its maximum size or scheduled time, the FortiAnalyzer 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 150.

If you display the log messages in formatted view, you can perform all the same actions as with the log message list. See “Viewing log messages” on page 138.

Figure 110: Log file list window



This page displays the following:

Delete	Select the file of files whose log messages you want to delete, then select *Delete*, and then select *OK* in the confirmation dialog box.
Display	Select the file whose log messages you want to view, then select *Display*, , to open the log message list. For more information, see "Viewing log messages" on page 138
Download	Download a log file. See "Downloading a log file" on page 149.
Import	Import log files. See "Importing a log file" on page 148.
Search	Search the log files by entering a text value in the search window, such as a device serial number.
Log file list	A list of the log files.
Device	The device host name.
Type	The log type. For example: *Email Filter*, *Event*, *Traffic*, *Web Filter*, *Network Scan*, *Virus*, *Application Control*, or *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 FortiAnalyzer unit to delete the original log files after uploading rolled logs to an FTP server, only the current log will exist.
From	The time when the log file began to be generated.

To	The time when the log file generation ended.
Size (bytes)	The size of the log file, in bytes.
Page navigation	Adjust the number of logs that are listed per page and browse through the pages.

Importing a log file

Imported log files can be useful when restoring data or loading log data for temporary use. For example, if you have older log files from a device, you can import these logs to the FortiAnalyzer unit so that you can generate reports containing older data.

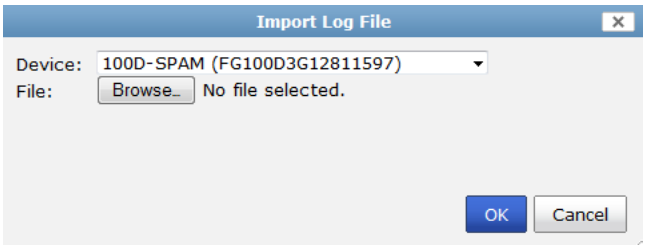
Importing log files is also useful when changing your RAID configuration. Changing your RAID configuration reformats the hard disk, erasing the log files. If you back up the log files, after changing the RAID configuration, you can import the logs to restore them to the FortiAnalyzer unit.

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 111: 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, select *Browse*. and find to the log file on the management computer.
5. Select *OK*.

   A message appears, stating that the upload is beginning, but will be cancelled if you leave the page.
6. Select *OK*.

   The upload time varies depending on the size of the file and the speed of the connection.

After the log file has been successfully uploaded, the FortiAnalyzer unit will inspect the file:

- If the `device_id` field in the uploaded log file does not match the device, the import will fail. Select *Return* to attempt another import.
- If you selected *[Take From Imported File]*, and the FortiAnalyzer unit's device list does not currently contain that device, a message appears after the upload. Select *OK* to import the log file and automatically add the device to the device list.

Downloading a log file

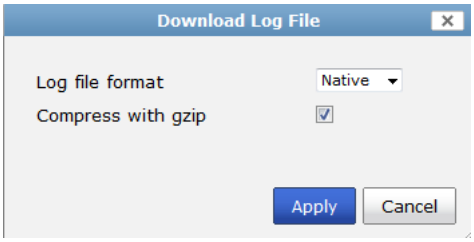
You can download a log file to save it as a backup or for use outside the FortiAnalyzer unit. The download consists of either the entire log file, or a partial log file, as selected by your current log view filter settings and, if downloading a raw file, the time span specified.

To download a log file:

1. Go to *Log View* > *Log Browse*.
2. Select the specific log file that you need to download, then select *Download* from the toolbar.

   The *Download Log File* dialog box opens.

   Figure 112: Download log file dialog box



3. Select the log file format, either text, Native, or CSV.
4. Select *Compress with gzip* to compress the log file.
5. Select *Apply* to download the log file.

   If prompted by your web browser, select a location to where save the file, or open the file without saving.

FortiClient logs

The FortiAnalyzer unit can receive FortiClient logs uploaded through TCP port 514. The FortiClient logs can be viewed and downloaded from *Log View* > *FortiClient*.

Figure 113: FortiClient logs

Download Search

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 Administration Guide*.

Configuring rolling and uploading of logs

You can control device log file size and use of the FortiAnalyzer unit's disk space by configuring log rolling and scheduled uploads to a server.

As the FortiAnalyzer 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 FortiAnalyzer 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*. For more information, see "Device log settings" on page 121. Log rolling and uploading can also be enabled and configured using the CLI. For more information, see the *FortiAnalyzer CLI Reference*.

Rolling and uploading CLI configuration

To enable or disable log file uploads:

To enable log uploads, enter the following CLI commands:

```
config system log settings
  config rolling-regular
    set upload enable
    end
  end
```

To disable log uploads, enter the following CLI commands:

```
config system log settings
  config rolling-regular
    set upload disable
    end
  end
```

To roll logs when they reach a specific size:

Enter the following CLI commands:

```
config system log settings
  config rolling-regular
    set file-size <integer>
    end
  end
```

where <integer> is the size at which the logs will roll, in MB.

To roll logs on a schedule:

To disable log rolling, enter the following CLI commands:

```
config system log settings
  config rolling-regular
    set when none
    end
  end
```

To enable daily log rolling, enter the following CLI commands:

```
config system log settings
  config rolling-regular
    set upload enble
    set when daily
    set hour <integer>
    set min <integer>
    set file-size <integer>
    end
  end
```

where:

hour <integer>	The hour of the day when the when the FortiAnalyzer rolls the traffic analyzer logs.
min <integer>	The minute when the FortiAnalyzer 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 FortiAnalyzer rolls the traffic analyzer logs.
`hour <integer>`	The hour of the day when the when the FortiAnalyzer rolls the traffic analyzer logs.
`min <integer>`	The minute when the FortiAnalyzer rolls the traffic analyzer logs.

Reports

FortiAnalyzer units can analyze information collected from the log files of managed log devices. It then presents the information in tabular and graphical reports that provide a quick and detailed analysis of activity on your networks.

To reduce the number of reports needed, reports are independent from devices, and contain layout information in the form of a report template. The devices, and any other required information, can be added as parameters to the report at the time of report generation.

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

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.

The *Reports* tab is available when the FortiAnalyzer operation mode is *Analyzer* only.

This chapter contains the following sections:

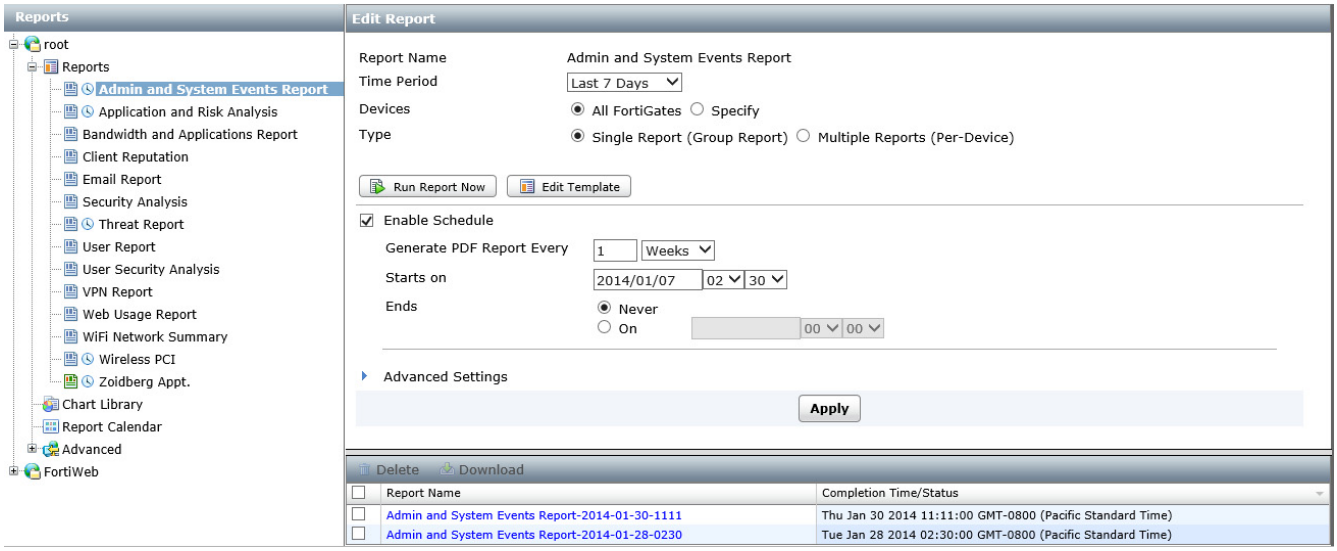
- Reports
- Report templates
- Report cover pages
- Chart library
- Report calendar
- Advanced

Reports

The FortiAnalyzer has 13 preconfigured reports and report templates for FortiGate log devices. FortiMail and FortiWeb log devices each have one default report. These report templates can be used as is, or you can clone and edit the templates. You can also create new reports and report templates that can be customized to your requirements.

In the *Reports* tab, go to *Reports* > *[report]* to view and configure the report settings, template, and schedule. The currently running reports and completed reports are shown in the lower content pane, see "Completed reports" on page 165.

Figure 114: Report page



The following information and settings are available in the *Edit Report* pane:

Report Name	The report template name.
Time Period	The time period that the report will cover. Select a time period, or select *Other* to manually specify the start and end date and time.
Devices	The devices that the report will include. Select either *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)*. This option is only available if multiple devices are selected.
Run Report Now	Select to immediately run the current report. See "Run a report" on page 162.
Edit Template	Select *Edit Template* to edit the report template including headings, images, charts, and report settings. See "Report templates" on page 166.
Enable Schedule	Select to enable schedules for the report selected. See "Schedules" on page 163.

Advanced Settings	Configure advanced report settings, such as filters and print options. See “Advanced settings” on page 163.
Complete Reports	The completed reports list. See “Completed reports” on page 165.

Right-clicking on a template in the tree menu opens a pop-up menu with the following options:

Report	
Create New	Create a new report. See “To create a new report:” on page 161.
Clone	Clone the selected report. See “To clone a report:” on page 162.
Delete	Delete the report. The default reports cannot be deleted. See “To delete a report:” on page 162.
Import	Import a report. See “Import and export” on page 176.
Export	Export a report. See “Import and export” on page 176.
Go To Template	Go to the report template. See “Report templates” on page 166.
Folder	
Create New	Create a new report folder. See “To create a new report folder:” on page 162.
Rename	Rename a report folder. See “To rename a report folder:” on page 162.
Delete	Delete a report folder. Any report templates in the folder will be deleted. See “To delete a report folder:” on page 162.

Default reports

The following tables list the default report templates and the charts they contain.

Table 6: FortiGate report templates

Report Template	Charts
Admin and System Events Report	• Admin Login And System Events • System Activity Summary
Application and Risk Analysis	• Top 20 Users By Bandwidth • Top 20 Users or Sources By Sessions • Top Users By Reputation Score (Bar Chart) • Top Devices By Reputation Scores • Application Category by Bandwidth (Pie Chart) • Top 30 Application Categories By Bandwidth • Application Risk Distribution • Number of Applications By Risk Behavior • High Risk Applications • Key Applications Crossing The Network • Applications Running Over HTTP • Top Web Categories By Session and Bandwidth (Pie Chart) • Top 20 Web Categories By Session and Bandwidth • Top Web Domains By Visits • Top Destination Countries by Browsing Time • Top Websites By Browsing Time • Top IPS Events by Severity • Top Critical IPS Events • Top High IPS Events • Top Medium IPS Events • Top Low IPS Events • Top Info IPS Events • Top 20 Viruses • Top 20 Virus Victims • Virus Discovered • Vulnerabilities Discovered • Data Leak Prevention Events
Bandwidth and Applications Report	• Bandwidth Summary for Past 7 Days • Session Summary For Past 7 Days • Traffic Statistics • Top 30 Applications by Bandwidth and Sessions • Application Categories by Bandwidth • Top 30 Users by Bandwidth and Sessions • Active Users for Past 7 days • Top 30 Destinations by Bandwidth and Sessions

Table 6: FortiGate report templates (continued)

Report Template	Charts
Client Reputation	• Score Summary For All Users and Devices • Top Users By Reputation Score • Top Users With Increased Scores • Top Incidents For Past 7 Days • Top Devices By Reputation Scores • Top Devices By Increased Scores
Email Report	• Top Email Senders • Top Email Recipients • Top Senders By Aggregated Email Size • Top Recipients By Aggregated Email Size

Table 6: FortiGate report templates (continued)

Report Template	Charts
Security Analysis	Bandwidth and Applications • Bandwidth Summary for Past 7 Days • Session Summary for Past 7 Days • Top Users By Bandwidth • Top Application By Bandwidth • Top Destination Addresses By Bandwidth • Top Users By Sessions • Top Application By Sessions • Top Destination Addresses By Sessions • DHCP Summary By Interfaces • Top WiFi Clients By Bandwidth • Traffic History By Active Users Web Usage • Top Web Users By Blocked Requests • Top Web Users By Allowed Requests • Top Web Users by Bandwidth • Top Web Users By Browsing Time • Top Blocked Web Sites • Top Allowed Web Sites • Top Allowed Web Sites By Bandwidth • Top Web Domains By Browsing Time Emails • Top Email Senders • Top Email Recipients • Top Senders By Aggregated Email Size • Top Recipients By Aggregated Email Size Threats • Top Viruses • Top Virus Victims • Top Attack Sources • Top Attack Victims VPN Usage • Top Site-to-Site IPsec Tunnels By Bandwidth • Top SSL VPN Tunnel Users By Bandwidth • Top Dial-up IPsec Tunnels By Bandwidth • Top SSL VPN Web Portal Users By Bandwidth • Top Dial-up VPN Users By Duration • VPN Traffic Usage Trend Admin and System Events • Admin Login And System Events • System Activity Summary User Activity Summary • Top 5 Users By Bandwidth

Table 6: FortiGate report templates (continued)

Report Template	Charts
Threat Report	Malware • Top Malware • Top Virus Victims • Malware Source • Virus Time Line Botnets • Detected Botnet • Botnet Victims • Botnet Sources • Botnet Timeline Intrusions • Top Attacks Detected • Top Attack Victims • Top Attack Sources • Attacks By Severity • Top Blocked Attacks • Attack Events For Past 7 Days
User Report	• Top 5 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
VPN Report	VPN Usage • VPN Traffic Usage Trend • Top Dial-up VPN Users By Duration SSL VPN • Top SSL VPN Sources By Bandwidth • Top SSL VPN Tunnel Users By Bandwidth • Top SSL VPN Web Portal Users By Bandwidth IPsec VPN • Top IPsec VPN Dial-up User By Bandwidth • Top Site-to-Site IPsec Tunnels By Bandwidth • Top Dial-up IPsec Tunnels By Bandwidth

Table 6: FortiGate report templates (continued)

Report Template	Charts
Web Usage Report	Web Usage Summary • Web Activity Summary for Past 7 Days • Browsing Time Summary for Past 7 Days • Bandwidth Summary for Past 7 Days Web Activity • Top Web Users By Request • Top Allowed Web Categories • Top Allowed Websites By Requests Web Browsing • Top Users By Estimated Browsing Time • Top 10 Categories • Top 50 Sites By Browsing Time Internet Bandwidth Usage • Top 20 Bandwidth Users • Top 20 Categories By Bandwidth • Top 50 Sites (and Category) by Bandwidth Most Blocked • Top Web Users By Blocked Requests • Top Blocked Web Categories • Top Blocked Web Sites
WiFi Network Summary	Network Summary • Data Transferred via WiFi • Number Of Distinct WiFi Clients Wireless Usage and Clients • Top APs by Bandwidth • Top SSIDs by Bandwidth • Top Applications via WiFi By Bandwidth • Top OS By Bandwidth • Top Device Type By Bandwidth • Top APs By Number of Clients • Top SSIDs By Number of Clients • Top WiFi Clients By Bandwidth • Top OS By Number of Clients • Top Device Types By Number of Clients
Wireless PCI	• On Wire AP Detection Summary By Status (Pie Chart) • Off Wire AP Detection Summary By Status (Pie Chart) • On Wire AP Detection Summary By Status • Off Wire AP Detection Summary By Status • Top 3 Managed AP Summary • Top Managed AP Summary • Top On Wire AP Details • Top Off Wire AP Details • Wireless Client Details

Table 7: Other report templates

Report Template	Charts
FortiMail	
FortiMail Default Report	• Fml History Top10 Client IP • Fml History Top10 Sender • Fml History Top10 Virus Sender • Fml History Top10 Local User • Fml History Top10 Recipient • Fml History Top10 Virus Recipient
FortiWeb	
FortiWeb Default Report	• Fwb Attack Top Attack Sources • Fwb Traffic Top Sources • Fwb Event Top Event Categories • Fwb Event Top Login By User • Fwb Attack Top Attacked Destinations • Fwb Traffic Top Destinations • Fwb Event Top Event Types

Configure reports

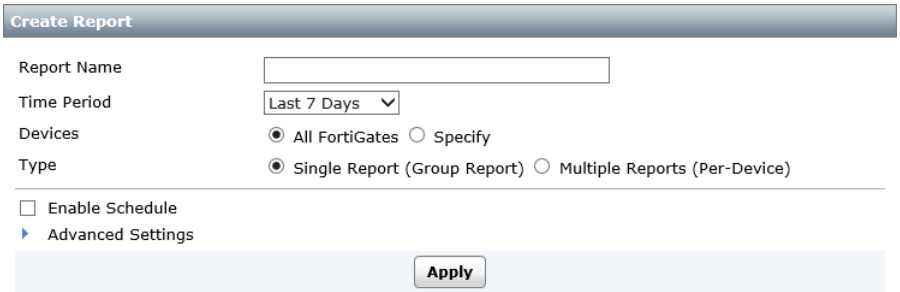
Reports and report templates can be created, edited, cloned, and deleted. You can also import and export report templates. New content can be added to and organized on a template, including: new sections, three levels of headings, text boxes, images, charts, and line and page breaks.

To create a new report:

1. In the *Reports* tab, right-click on *Reports* in the tree menu.
2. Under the *Report* heading, select *Create New*.

   The *Create Report* page opens.

   Figure 115: Create report page



3. Configure report settings. For more information see Figure 114 on page 154.

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. The *Edit Report* page opens for the new report.
5. Select *Edit Template* to edit the report template. See "Report templates" on page 166.
6. Configure the report schedule. For more information, see "Schedules" on page 163.
7. Configure advanced settings in the *Advanced Settings* section. See "Advanced settings" on page 163.
8. Select *Apply* to save the report template.

To clone a report:

1. Right-click on the report you would like to clone in the tree menu and select *Clone*.

   The *Clone Report Template* dialog box opens.
2. Enter a name for the new template, then select *OK*.

   A new template with the same information as the original template is created with the given name. You can then modify the cloned report as required.

To delete a report:

1. Right-click on the report template that you would like to delete in the tree menu, and select *Delete* under the *Report* heading.
2. In the confirmation dialog box, select *OK* to delete the report template.

Report folders

Report folders can be used to help organize your reports.

To create a new report folder:

1. In the *Reports* tab, right-click on *Reports* in the tree menu.
2. Under the *Folder* heading, select *Create New*.
3. In the *Create New Folder* dialog box, enter a name for the folder, and select *OK*.

   A new folder is created with the given name.

To rename a report folder:

1. Right-click on the report folder that you need to rename in the tree menu.
2. Under the *Folder* heading, select *Rename*.
3. In the *Rename Folder* dialog box, enter a new name for the folder, and select *OK*.

To delete a report folder:

1. Right-click on the report folder that you would like to delete in the tree menu, and select *Delete* under the *Folder* heading.
2. In the confirmation dialog box, select *OK* to delete the report folder.

Run a report

A report can be manually run at any time from the *Edit Report* window by selecting *Run Report Now*. You must specify at least one device to generate a report. If no devices are selected, a warning message will open.

The report will be generated and listed in the completed reports list in the lower content pane. See "Completed reports" on page 165 for information on viewing and managing generated reports.

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.

Report schedules can also be edited and disabled from the *Report Calendar*. See "Report calendar" on page 186 for more information.

Figure 116: Schedule a report template

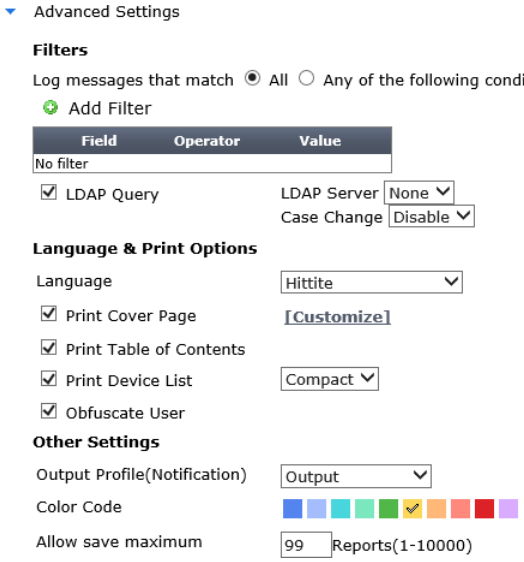
Configure the following settings:

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.
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.

Advanced settings

The advanced settings section allows you to configure filters, language and print options, and other settings.

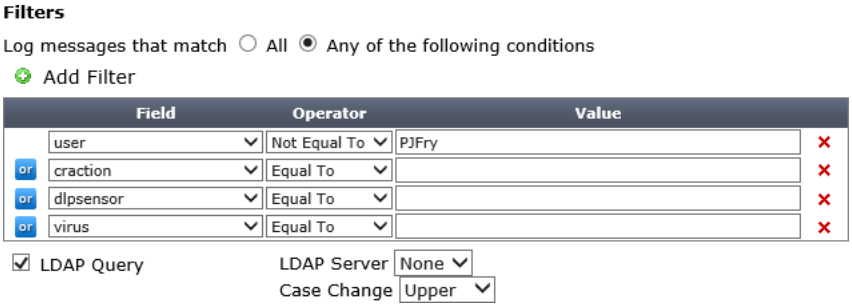
Figure 117: Advanced report settings



Filters

In the filters section of the *Edit Report* page, you can create and apply log message filters, and add an LDAP query to the report.

Figure 118: Report filters



Configure the following settings:

Log messages that match	Select *All* to filter log messages based on all of the added conditions, or select *Any of the following conditions* to filter log messages based on any one of the conditions.
Add Filter	Select to add filters. For each filter, select the field, and operator from the drop-down lists, then enter or select the value as applicable. Filters vary based on device type.
LDAP Query	Select the checkbox to add an LDAP query, then select the LDAP server and the case change value from the drop-down lists.

Select *Apply* to apply any changes to the report.

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.

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 the checkbox to print the report cover page. Select *Customize* to customize the cover page. See “Report cover pages” on page 176.
Print Table of Contents	Select the checkbox to include a table of contents.
Print Device List	Select the checkbox to print the device list. Select *Compact*, *Count*, or *Detailed* from the drop-down list.
Obfuscate User	Select the checkbox to hide user information in the report.

Select *Apply* to apply any changes you have made.

Other settings

Other settings that can be configured include the output profile, the report color code, and the maximum number of reports that can be saved. See Figure 117 on page 163.

Output Profile (Notification)	Select the output profile from the drop-down list, or select *Create New* to create a new output profile. See "Output profile" on page 191.
Color Code	The color used to identify the report on the calendar. Select a color code to apply to the report schedule.
Allow save maximum	Select a value between 1-10000 for the maximum number of reports to save.

Select *Apply* to apply any changes you have made.

Completed reports

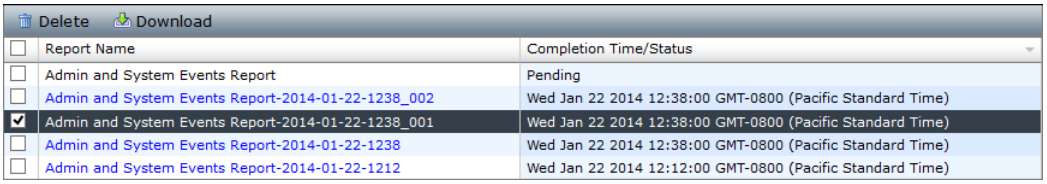
Competed reports are displayed in the lower content pane of the *Reports* tab. The report name and completion time or status are shown in the table. Selecting a report in the table will open the report in a new browser window or tab, from which you can also save the report as a PDF file.

The toolbar and the right-click menu provide options to delete or download the selected reports, as well as to run the report (see "Run a report" on page 162).

Completed reports can be viewed for specific devices from the *Device Manager* tab. See "To view device reports:" on page 166 or "Device reports" on page 54.

Completed reports can also be downloaded and deleted from the Report Calendar page. See "Report calendar" on page 186.

Figure 119: Completed reports



The following options are available:

Delete	Select one or more reports in the completed reports list, then select *Delete* from the toolbar or right-click menu. Select *OK* in the confirmation dialog box to delete the selected report or reports.
Download	Select one or more reports in the completed reports list, then select *Download* from the toolbar or right-click menu to download the selected report or reports. Each report will be saved individually as a PDF file on the management computer. Reports that are not done cannot be downloaded.
Select All	Select *Select All* from the right-click menu to select all the reports in the completed reports list.

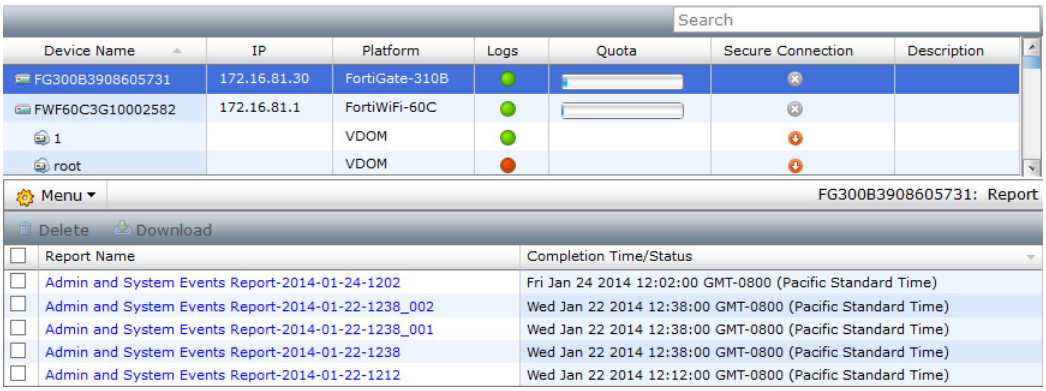
Report Name	The name of the report.
Completion Time/Status	The completion status of the report, or, if the report is complete, the data, and time (including time zone) that the report completed.

To view device reports:

1. In the *Device Manager* tab, select the ADOM that contains the device whose report you would like to view.

   All of the reports that have been run for the selected device are shown in the lower content pane.

   Figure 120: Device reports

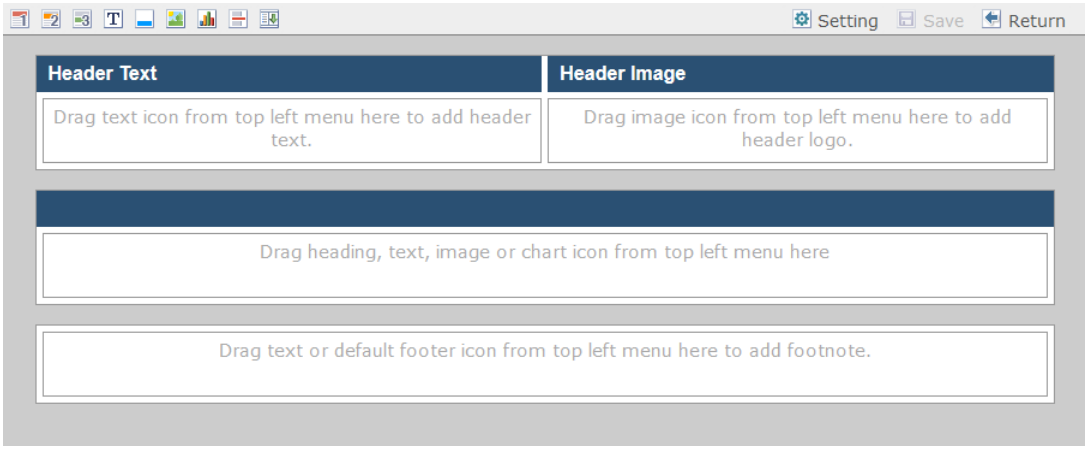


2. Select a report from the table to open it in a new browser window or tab, from which you can save the report as a PDF file.
3. Select one or more reports, then select *Delete* or *Download* to delete or download the selected reports. See “Delete” and “Download” on page 165, respectively.

Report templates

To configure report templates, in the *Reports* tab, select the report in the tree menu that you need to configure. Either right-click on the report in the tree menu and select *Go To Template*, or select *Edit Template* in the content pane.

Figure 121: Default new report template



Various content can be added to a report template, such as sections, charts, images, and typographic elements, using the template toolbar. The template color scheme, fonts, and layout can be controlled, and all the report sections and elements can be edited and customized as needed.

Workspace settings

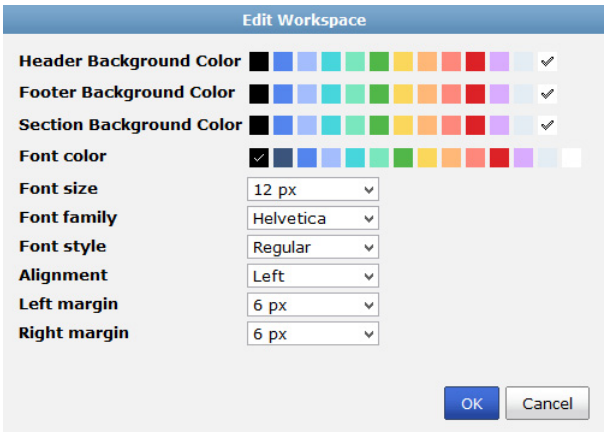
The report template workspace controls the colors, fonts, alignment, and margins of the report.

To edit the template workspace:

1. Select *Setting* in the template toolbar.

   The *Edit Workspace* window opens.

Figure 122: Edit workspace



2. Configure the following settings:

Header Background Color	Select the background color for the header from the palette.
Footer Background Color	Select the background color for the footer from the palette.
Section Background Color	Select the background color for sections 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.

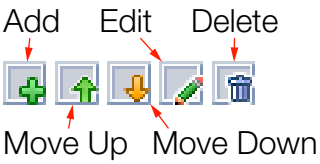
3. Select *OK* to apply your changes.

Sections

Report template sections contain all other report elements. By default, a blank report contains sections for header text, a header image, and a footer that cannot be removed. One blank section for content is included.

Elements can be added to, removed from, and organized in the blank section. Sections can be added, moved, edited, and removed using the section toolbar that appears when you hover the cursor over the section title bar, Figure 123.

Figure 123: Section toolbar



Add	Add a new section to the report template. See "To add a section to a report template:" on page 169.
Move Up	Move the section above the section currently directly above it.
Move Down	Move the section below the section currently directly below it.
Edit	Edit the section. See "To edit a section in a report template:" on page 169.
Delete	Delete the section. Select *OK* in the confirmation dialog box. All section content will also be deleted.

Section specific settings will overwrite the workspace settings if configured after the workspace. To revert to the workspace settings, reconfigure the workspace. See "Workspace settings" on page 167.

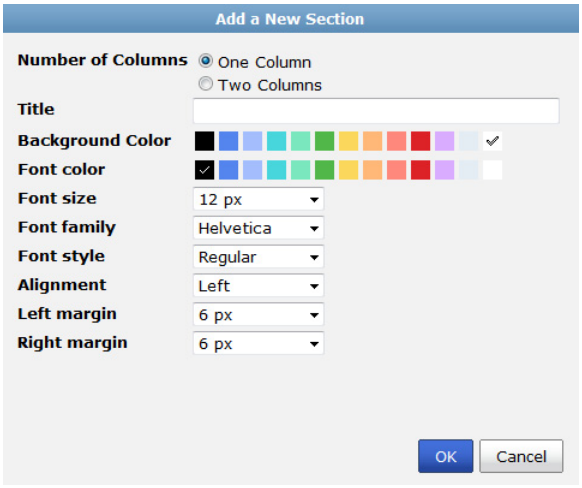
The header text and header image will print the cover page information, including the device hostname, in the report header when selecting not to print the report cover page from *Language & Print Options* (see "Language & print options" on page 164).

To add a section to a report template:

1. From any content section toolbar, select the *Add a New Section* icon,  .

   The *Add a New Section* dialog box opens.

   Figure 124: Add a new section



2. Configure the following settings:

Number of Columns	Select to the number of columns the section will have. Either one or two.
Title	Enter a title for the section (optional).
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 font families: *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.

3. Select *OK* to create the new section.

To edit a section in a report template:

1. From any content section toolbar, select the *Add Section* icon,  .

   The *Edit Section* dialog box opens. See Figure 124 on page 169.
2. Configure the section settings as required.
3. Select *OK* to edit the section.

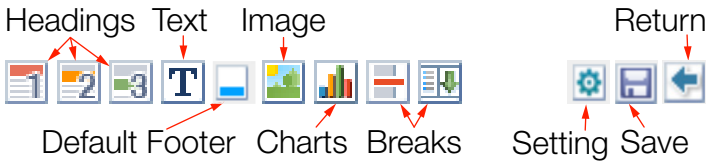
Elements

Elements can be added to sections in a report template by clicking and dragging the element's icon from the template toolbar to the location in the template where you want the element to appear.

The default sections will only accept certain elements:

- *Header Text* will only accept a single text element.
- *Header Image* will only accept a single image element.
- The footer section will only accept a single text element or the default footer element.

Figure 125: Template toolbar



Headings	Add one of three levels of headings to the template. See "Headings" on page 171.
Text	Add a text box to the template. See "Text boxes" on page 172.
Default Footer	The default footer can only be added to the footer or header text sections of the template. It includes the report name and the FortiAnalyzer host name.
Image	Add an image to the template. See "Images" on page 173.
Charts	Add a chart to the template.
Breaks	Add a line or page break to the template.
Settings	Adjust the template workspace. See "Workspace settings" on page 167.
Save	Save your template changes.
Return	Return to the *Edit Report* page. If you have not saved your template changes, a confirmation dialog box will ask you to confirm leaving the page.

Moving an element

To move an element that has already been placed in the template, simply click and drag the element to the new location. A gray box with a dashed red outline will appear in the location where the element will be placed.

If you accidently drag the element to a location where it does not fit, such as dragging an image into the footer section, the element will return to its previous location.

Deleting an element

To delete an element from the template, select delete icon, , in the element toolbar, then select *OK* in the confirmation dialog box.

Headings

Three heading levels are available and can be added to content sections within the report template. Heading settings, such as font and color, take precedence over section and workspace settings.

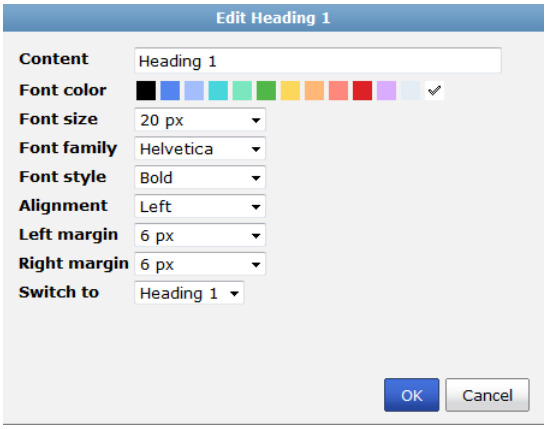
To add headings to a report template:

Click and drag the required heading icon ( ,  , or ) from the template toolbar to the location in the content section where you want to add the heading.

To edit headings:

1. Select the edit icon in the heading toolbar,  , to open the *Edit Heading* dialog box.

Figure 126: Edit heading dialog box



2. 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 the font family to use for the heading text.
Font style	Select the font style.
Alignment	Select the heading text alignment.
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. This will not change the font size, style, or color.

3. Select *OK* to apply your changes.

Text boxes

Text boxes can be added to content sections of the report template. A text box can also be added to the *Header Text* and footer sections if they contain no other elements.

When adding text to the report header or footer, you can only edit the content. Additional settings, such as color or font, are not available.

To add text to a report template:

Click and drag the text icon,  , from the template toolbar to the location in the section where you want to add text.

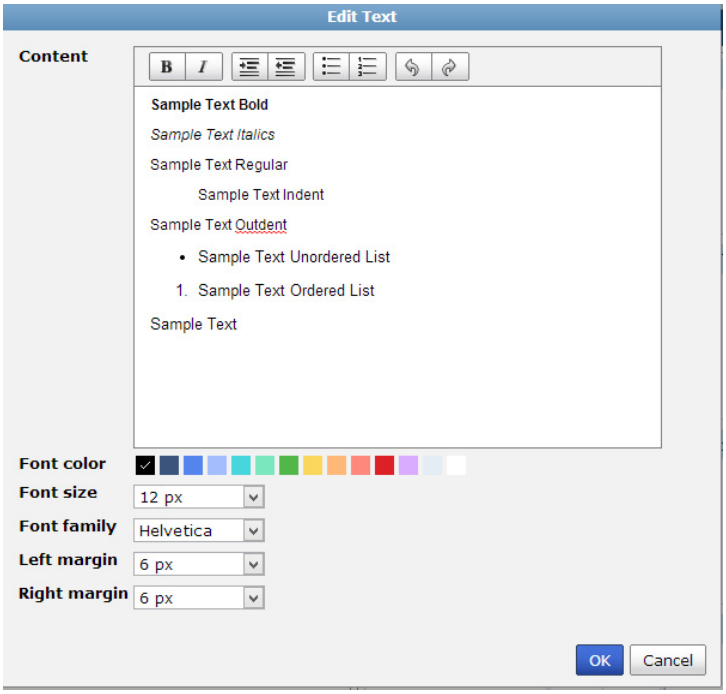
A single text box can be added to the *Header Text* Section and the footer section. Multiple text boxes can be added to content sections.

It is recommended that you edit the section prior to adding text elements as the section menu will override settings in an existing custom text section. See "Sections" on page 168.

To edit report template text:

1. Select the edit icon in the text box toolbar,  , or double-click on the text box, to open the *Edit Text* dialog box.

Figure 127: Edit text dialog box



2. 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, bulleted 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 the font family from the drop-down list.
Font style	Select the font style from the drop-down list.
Left margin	Select the left margin size from the drop-down list.
Right margin	Select the right margin size from the drop-down list.

3. Select *OK* to finish editing the text.

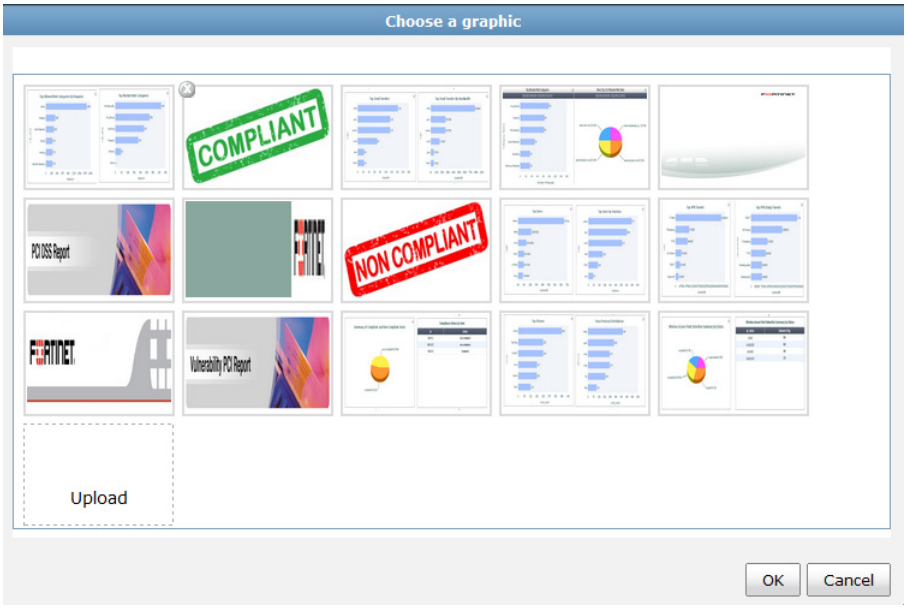
Images

A single image can be added to the *Header Image* section. Multiple images can be added to content sections.

To add an image to a report template:

1. 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 128: Choose a graphic dialog box



2. Select an image from the list, or select *Upload* to browse for an image on your computer.

3. Select *OK* to add the selected image to the report template.

   The image will appear in the location that you had selected in the template.

To edit an image:

1. Select the edit icon in the image toolbar, , or double-click on the image, to open the *Choose a graphic* dialog box.
2. Change the graphic as need, then select *OK*.

Charts

Chart elements can only be placed in content sections of the report template. The chart content can be filtered, and the chart content can be edited.

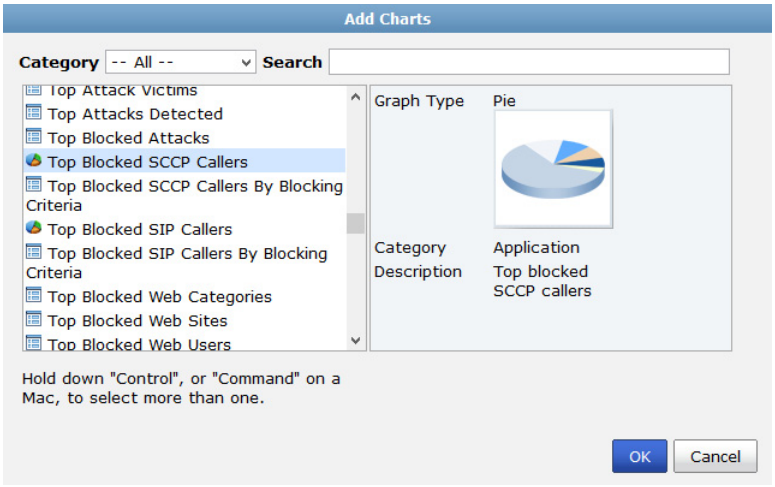
Predefined chart content cannot be changed. If attempting to edit a predefined chart, you will be prompted with a warning dialog box and given the option to clone the chart and make changes. The clone will replace the predefined chart in the report template.

To add a chart to a report template:

1. Click and drag the chart icon, , to the location where you want to add the chart.

   The *Add Charts* dialog box will open.

   Figure 129: Add a new chart



2. 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 from the *Category* drop-down list, 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.
3. Select *OK* once you have found and selected the chart you would like to add.

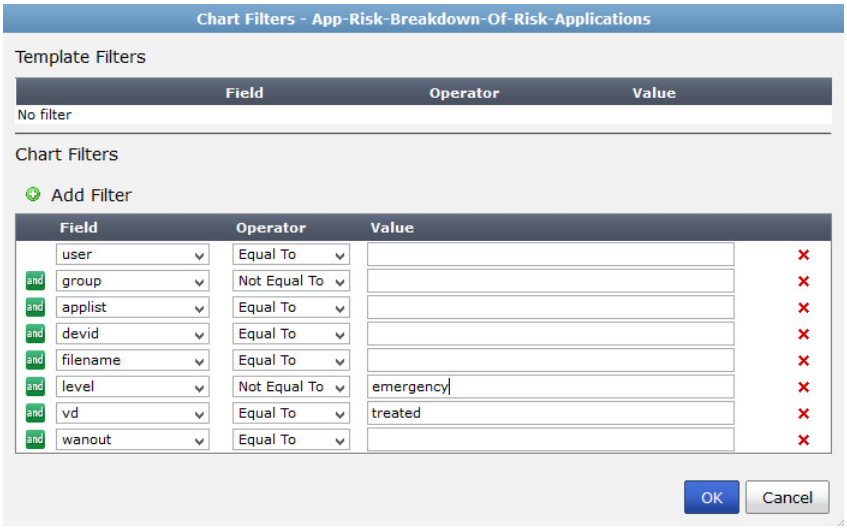
   The chart's placeholder will appear in the location that you had selected in the template.

To add a chart filter

1. Select the filter icon, , in the chart toolbar.

   The *Chart Filters* dialog box will open.

   Figure 130: Chart filters



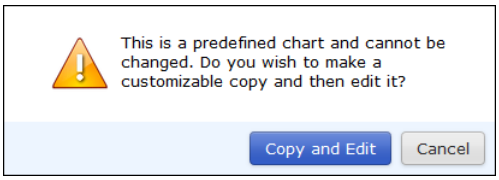
2. Add filters to the chart as needed.
3. Select *OK* to apply the filters to the chart and return to the template page.

To edit a chart:

1. Select the edit icon in the chart toolbar, , or double-click on the chart.

   If you are attempting to edit a predefined chart, a warning dialog box will open (Figure 131). Select *Copy and Edit* to continue editing a clone of the chart.

   Figure 131: Edit predefined chart



   The *Edit Chart* or *Clone Chart* (if editing a predefined chart) dialog box will open.
2. See “To edit a chart:” on page 185 for more information on editing and cloning charts.
3. Select *OK* to apply your changes.

Breaks

Two types of breaks can be added to the content sections of a report template: line breaks, and page breaks. Breaks can not be edited.

To add a break to a report template:

Click and drag the line break or page break icon (, or , respectively) to the location in a content section in the report template where you want to add the break.

Import and export

Report templates can be imported from and exported to the management computer.

To import a report template:

1. Right-click on *Reports*, and select *Import*.

   The *Import Report Template* dialog box opens.

2. Select *Browse*, locate the report template (.dat) file on your management computer, and select *OK*.

   The report template will be loaded into the FortiAnalyzer unit.

To export a report template:

1. Right-click on the report you would like to export in the tree menu and select *Export*.
2. If a dialog box opens, select to save the file (.dat) to your management computer, and select *OK*.

   The report template can now be imported to another FortiAnalyzer device.

Report cover pages

The report cover page is only included in the report when enabled in the language and print options. See “Language & print options” on page 164.

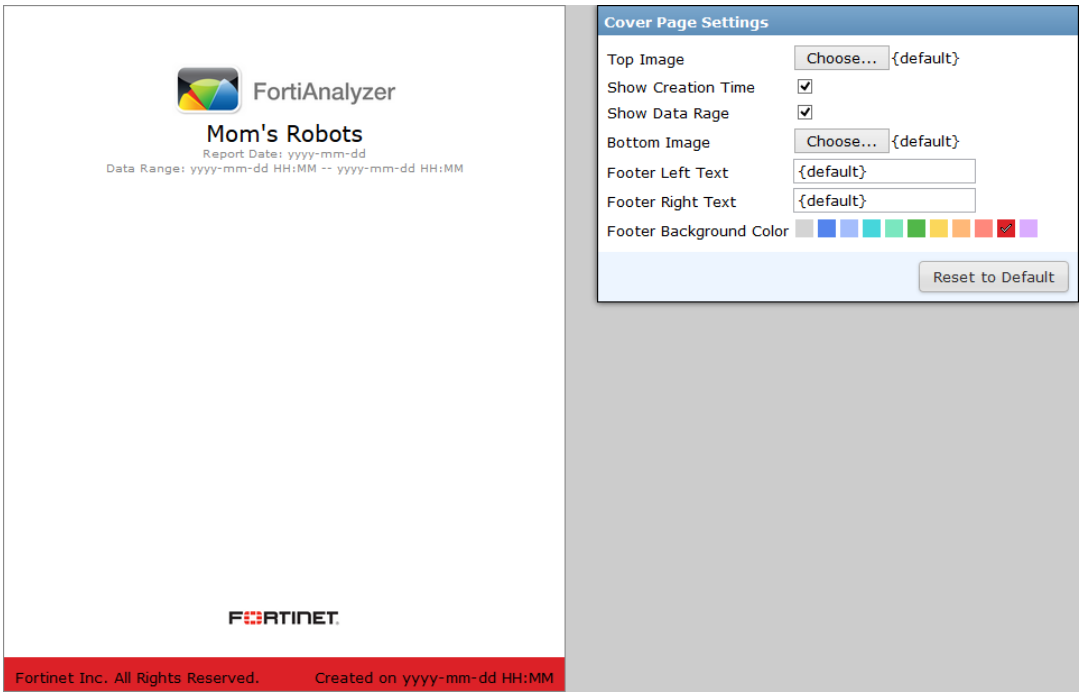
When enabled, the cover page can be edited to contain the desired information and imagery.

To edit cover page settings:

1. In the *Reports* tab, select the report in the tree menu whose cover page you are editing.
2. In the *Advanced Settings* section, select *Customize* in the *Language & Print Options* section.

   The *Cover Page Settings* page opens.

Figure 132: Cover page settings



3. Configure the following settings:

Top Image	Select *Choose* to open the *Choose a graphic* dialog box (Figure 128). Select an image, or select *Upload* to find an image on the management computer, then select *OK* to add the image at the top of the cover page.
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 open the *Choose a graphic* dialog box (Figure 128). Select an image, or select *Upload* to find an image on the management computer, then select *OK* to add the image at the bottom of the cover page.
Footer Left Text	Edit the text printed in the left hand footer of the cover page.
Footer Right Text	Edit the text printed in the left hand footer of the cover page. `{default}` prints the report creation date and time.
Footer Background Color	Select the cover page footer background color from the palette.
Reset to Default	Select to reset the cover page settings to their default settings.

4. Select *Save* in the toolbar, to save your changes.
5. Select *Return* in the toolbar, to return to *Edit Report* page.

Chart library

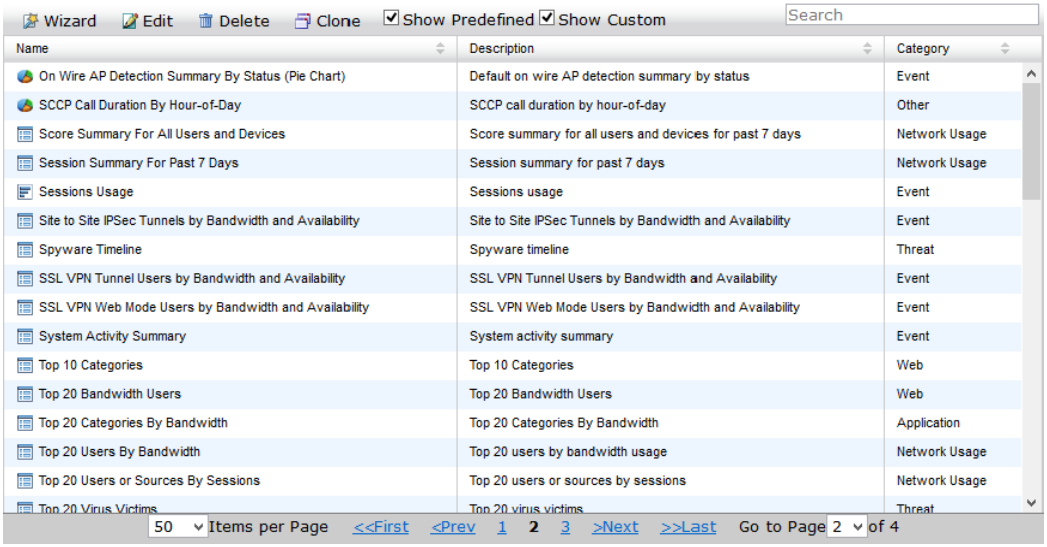
The FortiAnalyzer unit provides a selection of predefined charts. New charts can be created using the custom chart wizard, by cloning and editing an existing chart, or by using the advanced chart creation option. You can select to display predefined chart, custom charts, or both.

For advanced users, right-click the right content pane and select *Create New* to create SQL based charts. See “To create a new chart:” on page 183.

Charts are predefined to show specific information in an appropriate format, such as pie charts or tables. They are organized into categories, and can be added to, removed from, and organized in reports.

To view the chart library, go to *Reports* > *Chart Library*.

Figure 133: Chart library



The following options and information is available:

Wizard	Launch the custom chart wizard. This option is only available for FortiGate and FortiCarrier ADOMs. See “Custom chart wizard” on page 179.
Create New	Create a new chart. For FortiGate and FortiCarrier ADOMs, this option is only available from the right-click menu. See “To create a new chart:” on page 183.
Edit	Select to edit a chart. This option is only available for custom charts. See “To edit a chart:” on page 185.
View	Select to view chart details. This option is only available for predefined charts, as they cannot be edited.
Delete	Select to delete a chart. This option is only available for custom charts. See “To delete charts:” on page 185.
Clone	Select to clone an existing chart. See “To clone a chart:” on page 184.
Show Predefined	Select to display predefined charts.

Show Custom	Select to display custom charts.
Search	Enter a search term in the search field to find a specific chart.
Page navigation	Adjust the number of logs that are listed per page and browse through the pages.

Custom chart wizard

The custom chart wizard is a step by step guide to help you create custom charts. It is only available for FortiGate and FortiCarrier ADOMs.

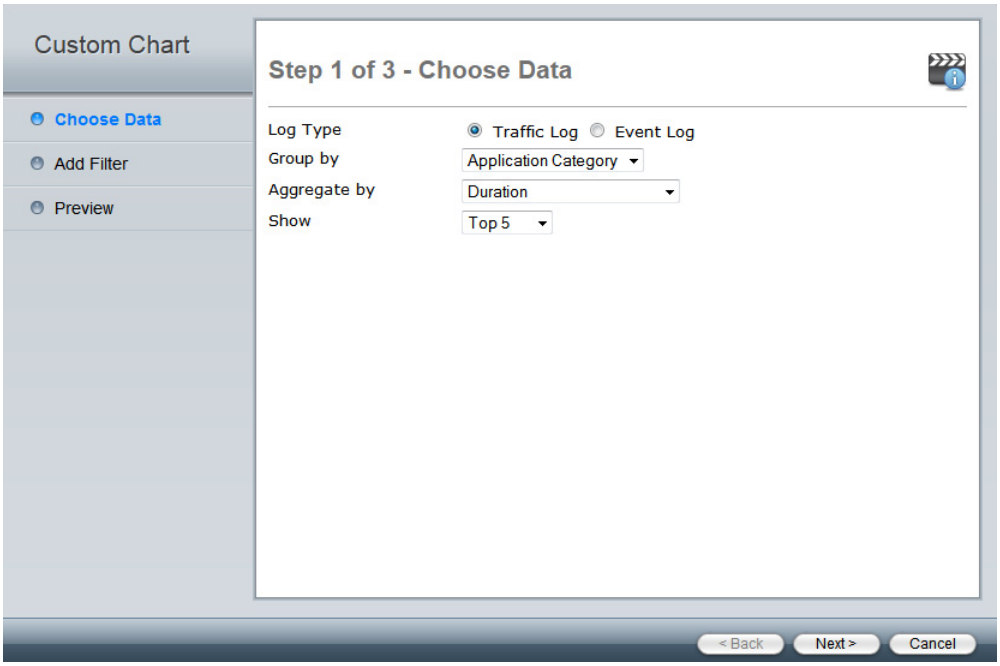
To start the custom chart wizard, go to *Reports* > *Chart Library*, and select *Wizard* in the toolbar. Follow the steps in the chart wizard, outlined below, to create a custom chart.

Select the *Tutorial* icon, , on any of the wizard windows to view the online chart wizard video.

Step 1 of 3 - Choose data

Configure the data that the custom chart will use.

Figure 134: Choose data



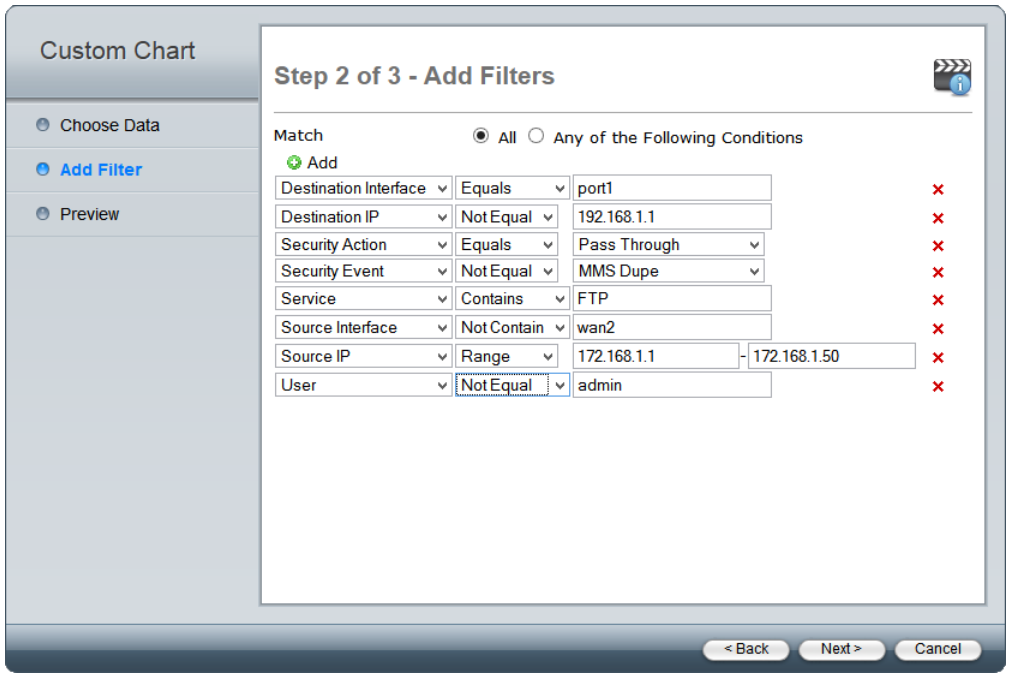
Configure the following settings, then select Next to proceed to the next step:

Log Type	Select either *Traffic Log* or *Event Log*.
Group by	Select how the data are grouped. Depending on the chart type selected in step 3, this selection will relate to *Column 1* (Table), the *Y-axis* (Bar and Line graphs), or the *Legend* (Pie chart). See "Step 3 of 3 - Preview" on page 182. The available options will vary depending on the selected log type: • Traffic log: *Application Category, Application ID, Application Name, Attack, Destination Country, Destination Interface, Destination IP, Device Type, Source Interface, Source IP, Source SSID, User, Virus, VPN, VPN Type, Web Category*, or *Website (Hostname)*. • Event log: *VPN Tunnel*, or *Remote IP*.
Aggregate by	Select how the data is aggregated. Depending on the chart type selected in step 3, this selection will relate to *Column 2* (Table), the *X-axis* (Bar and Line graphs), or the *Value* (Pie chart). See "Step 3 of 3 - Preview" on page 182. The following options are available: *Duration*, *Received Bytes*, *Sent Bytes*, *Total Bytes*, *Total Sessions* or *Total Blocked Sessions* (Traffic log only).
Show	Select how much data to show in the chart from the drop-down list. One of the following: *Top 5, Top 10, Top 25, Top 50*, or *Top 100*.

Step 2 of 3 - Add filters

You can add one or more filters to the chart. These filters will be permanently saved to the dataset query.

Figure 135: Add filters page



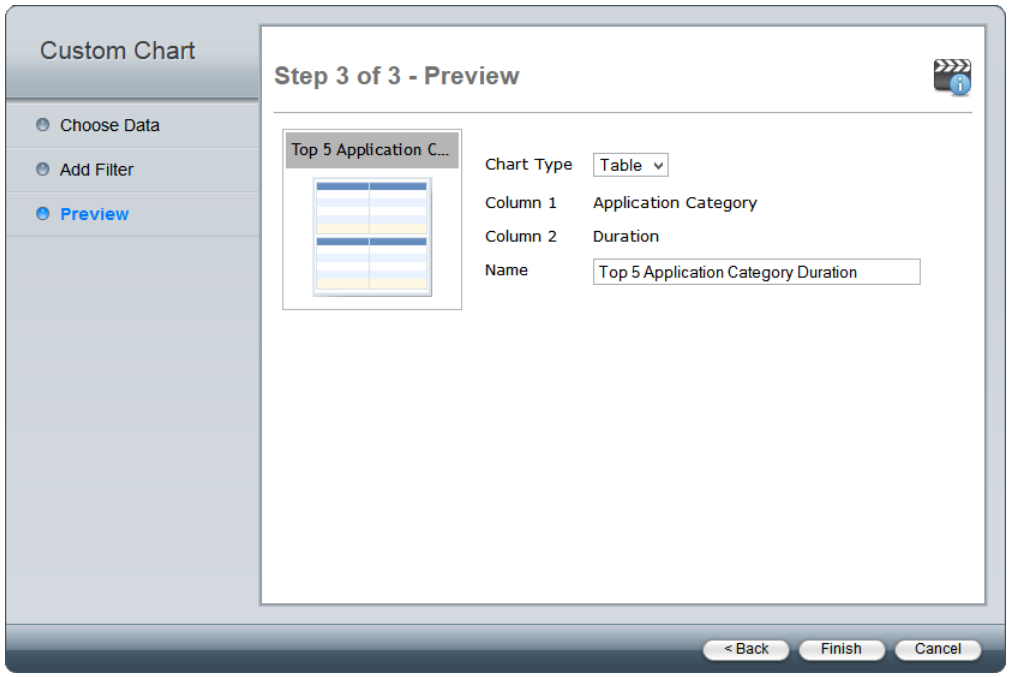
Configure the following settings:

Match	Select *All* to filter data based on all of the added conditions, or select *Any of the Following Conditions* to filter the data based on any one of the conditions.
+ Add	Select to add filters. For each filter, select the field, and operator from the drop-down lists, then enter or select the value as applicable. Filters vary based on device type. The available filters vary depending on the log type selected. Select the delete icon,  , to remove a filter.
Destination Interface	This filter is available for traffic logs only. The available operators are: *Equals*, *Not Equal*, *Contains*, and *Not Contain*.
Destination IP	This filter is available for traffic logs only. The available operators are: *Equals*, *Not Equal*, and *Range*. If *Range* is selected, enter the starting and ending IP address in the value fields.
Security Action	This filter is available for traffic logs only. The available operators are: *Equals* and *Not Equal*. The value is always *Pass Through*.
Security Event	Select *Equals or Not Equal* from the second drop-down list. Select one of from the third drop-down list. Select the garbage can icon to delete the filter. This filter is available for traffic logs only. The available operators are: *Equals* and *Not Equal*. The value can be one of the following, selected from the drop-down list: *Analytics*, *Application Control*, *AV Error*, *Banned Word*, *Command Block*, *DLP*, *File Filter*, *General Mail Log*, *HTML Script Virus*, *IPS*, *MIME Fragmented*, *MMS Checksum*, *MMS Dupe*, *MMS Endpoint*, *MMS Flood*, *MAC Quarantine*, *Oversize*, *Script Filter*, *Spam Filter*, *SSH Block*, *SSH Log*, *Switching Protocols*, *Virus*, *VOIP*, *Web Content*, *Web Filter*, or *Worm*.
Service	This filter is available for both traffic and event logs. The available operators are: *Equals*, *Not Equal*, *Contains*, and *Not Contain*.
Source Interface	This filter is available for traffic logs only. The available operators are: *Equals*, *Not Equal*, *Contains*, and *Not Contain*.
Source IP	This filter is available for traffic logs only. The available operators are: *Equals*, *Not Equal*, and *Range*. If *Range* is selected, enter the starting and ending IP address in the value fields.
User	This filter is available for both traffic and event logs. The available operators are: *Equals*, *Not Equal*, *Contains*, and *Not Contain*.

Step 3 of 3 - Preview

The preview page allows you to select the chart type and rename the custom chart.

Figure 136: Preview page



Configure the following settings:

Chart Type	Select the chart type in the drop-down list; one of the following: *Bar*, *Line*, *Pie*, or *Table*. ***Note:*** Depending on the chart settings configured in the previous two steps, the available options may be limited.
Column 1 / Y-axis / Legend	Displays the *Group by* selection. See "Group by" on page 180. The field varies depending on the chart type.
Column 2 / X-axis / Value	Displays the *Aggregate by* selection. See "Aggregate by" on page 180. The field varies depending on the chart type.
Name	Displays the default name of the custom chart. This field can be edited.

Select *Finish* to finish the wizard and create the custom chart. The custom chart will be added to the chart table and will be available for use in report templates.

Managing charts

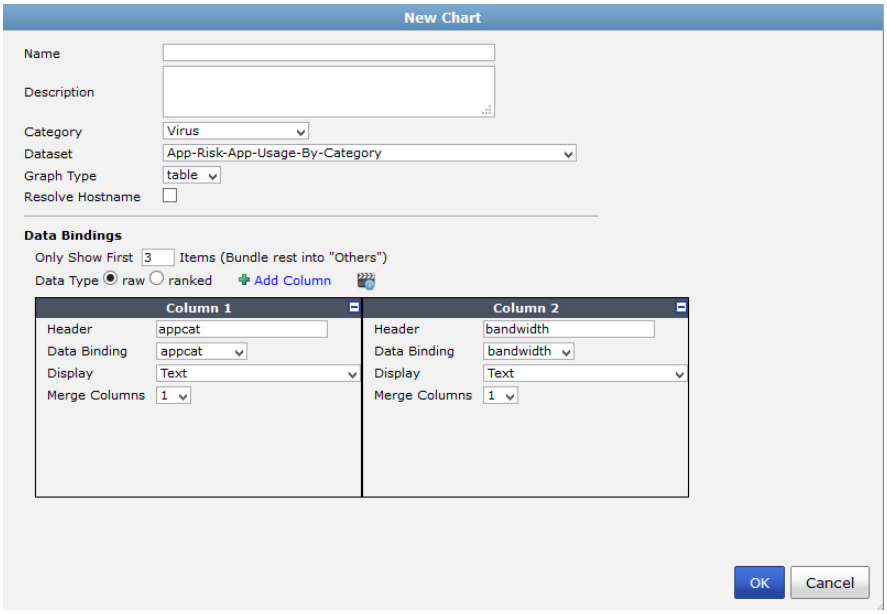
Predefined charts can be viewed and cloned. Custom charts can be created, edited, cloned, and deleted.

To create a new chart:

1. In the chart library:
   - If you are creating a chart in a FortiGate or FortiCarrier ADOM: right-click in the content pane and select *Create New*.
   - If you are creating a chart in any other ADOM: select *Create New* in the toolbar.

   The *New Chart* dialog box opens.

Figure 137: Create new chart



Select the *Tutorial* icon, , to view the online chart creation video.

2. Enter the required information for the new chart.

Name	Enter a name for the chart.
Description	Enter a description of the chart.
Category	Select a category for the chart from the drop-down list; one of: *FortiMail*, *Other*, *Event*, *Threat*, *FortiWeb*, *Email*, *VPN*, *Application*, *Network Usage*, *Web*, or *DLP*.
Dataset	Select a dataset from the drop-down list. See "Dataset" on page 187 for more information. The options will vary based on device type.
Graph Type	Select a graph type from the drop-down list; one of: *table*, *bar*, *pie*, or *line*. This selection will affect the rest of the available selections.
Line Subtype	Select one of the following options: *basic*, *stacked*, or *back-to-back*. This option is only available when creating a line graph.
Resolve Hostname	Select to resolve the hostname.

Data Bindings	The data bindings vary depending on the chart type selected.
bar, pie, or line graphs	
X-Axis	*Data Binding*: Select a value from the drop-down list. The available options will vary depending on the selected dataset. *Only Show First*: Enter a numerical value. Only the first 'X' items will be displayed. Other items are bundled into the *Others* category. *Overwrite label*: Enter a label for the axis.
Y-Axis	*Data Binding*: Select a value from the drop-down list. The available options will vary depending on the selected dataset. *Overwrite label*: Enter a label for the axis. *Group by*: Select a value from the drop-down list. The available options will vary depending on the selected dataset. This option is only available when creating a bar graph.
Order By	Select to order by the X-Axis or Y-Axis. This option is only available when creating a line or bar graph.
table	
Only Show First Items	Enter a numerical value. Only the first 'X' items will be displayed. Other items are bundled into the *Others* category. This option is available for all columns when *Data Type* is set to *raw*. When *Data Type* is set to ranked, this option is available in *Column 1*.
Data Type	Select either *ranked* or *raw*.
Add Column	Select to add a column.
Columns	Up to fifteen columns can be added. The following column settings must be set: • *Header*: Enter header information. • *Data Binding*: Select a value from the drop-down list. The options vary depending on the selected dataset. • *Display*: Select a value from the drop-down list. • *Merge Columns*: Select a value from the drop-down list. This option is only available when *Data Type* is *raw*. If applicable, enter a *Merge Header*. • *Order by this column*: Select to order the table by this column. This option is only available in *Column 1* when *Data Type* is *ranked*.

3. Select *OK* to create the new chart.

To clone a chart:

1. In the chart library, select the chart that you would like to clone and select *Clone*,  , from either the toolbar or right-click menu.

   The *Clone Chart* dialog box opens.
2. Edit the information as needed, then select *OK* to clone the chart.

To edit a chart:

1. In the chart library, double-click on the custom chart you need to edit, or select the chart then select *Edit*,  , from either the toolbar or right-click menu.

   The *Edit Chart* dialog box opens.
2. Edit the information as required, then select *OK* to finish editing the chart.

Predefined charts cannot be edited, the information is read-only. A predefined chart can be cloned, and changes can then be made to said clone. See "To clone a chart:" on page 184.

To delete charts:

1. In the chart library, select the custom chart or charts that you would like to delete and select *Delete*,  , from either the toolbar or right-click menu.
2. Select *OK* in the confirmation dialog box to delete the chart or charts.

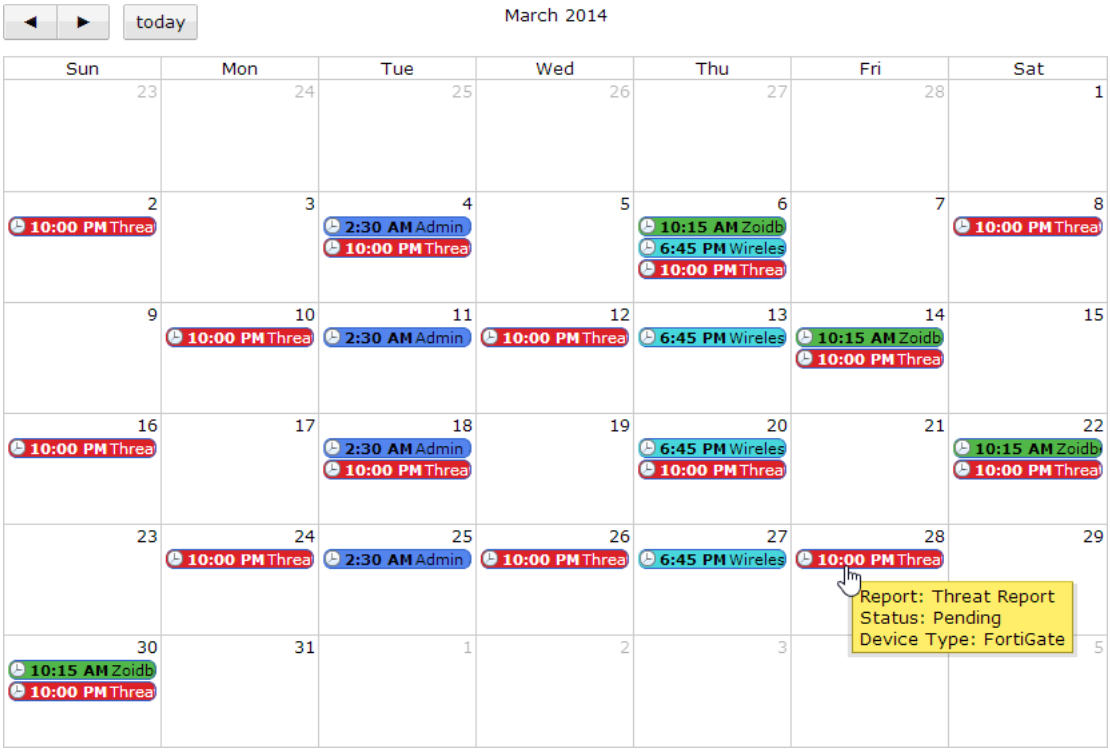
Predefined charts cannot be deleted.

Report calendar

The report calendar provides an overview of scheduled reports. You can view all reports scheduled for the selected month. From the calendar page, you can edit and disable upcoming reports, and delete or download completed reports.

To view the report calendar, go to *Reports* > *Report Calendar*.

Figure 138: Report calendar



Hovering the mouse cursor over a scheduled report on the calendar opens a notification box that shows the report's name and status, as well as the device type.

Selecting the left and right arrows at the top of the calendar page will adjust the month that is shown. Select *Today* to return to the current month.

To edit a report schedule:

1. Right-click on the scheduled report in the report calendar and select *Edit*.

   The *Edit Report* window will open. See Figure 114 on page 154.
2. Edit the report settings as required, then select *Apply* to apply the changes.

To disable a scheduled report:

1. Right-click the scheduled report and select *Disable* from the right-click menu.
2. In the confirmation box, select *OK*.

   Disabling a report will remove all scheduled instances of the report from the report calendar. Completed reports will remain in the report calendar.

To delete a scheduled report:

1. Right-click the scheduled report that you would like to delete and select *Delete*.

   Only scheduled reports that have already been run can be deleted.
2. Select *OK* in the confirmation dialog box to delete the scheduled report.

To download a report:

1. Right-click the scheduled report that you would like to download and select *Download*.

   Only scheduled reports that have already been run can be downloaded.
2. Depending on your web browser and management computer settings, save the file to your computer, or open the file in an applicable program.

   Reports are downloaded as PDF files.

Advanced

The advanced menu allows you to view, configure and test datasets, create output profiles, and manage report languages.

Dataset

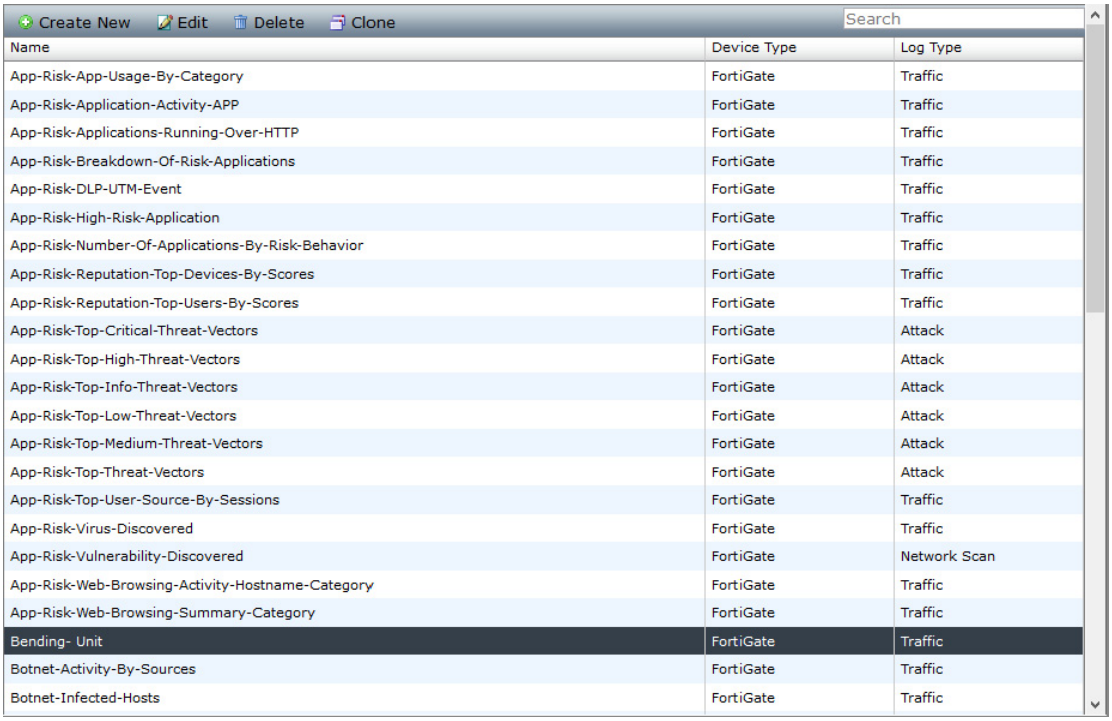
FortiAnalyzer datasets are collections of log files from monitored devices. Reports are generated based on these datasets.

Predefined datasets for each supported device type are provided, and new datasets can be created and configured. Both predefined and custom datasets can be cloned, but only custom datasets can be deleted. You can also view the SQL query for a dataset, and test the query against specific devices or log arrays.

FortiAnalyzer v5.0 Patch Release 5 introduced new datasets for SIP and SCCP. FortiAnalyzer v5.0 Patch Release 6 introduces new datasets for Botnet (Botnet-Activity-By-Sources, Botnet-Infected-Hosts, Botnet-Sources, Botnet-Timeline, and Detected-Botnet).

To view and configure datasets, go to *Reports* > *Advanced* > *Dataset* in the tree menu.

Figure 139: Datasets



The following options and information are available:

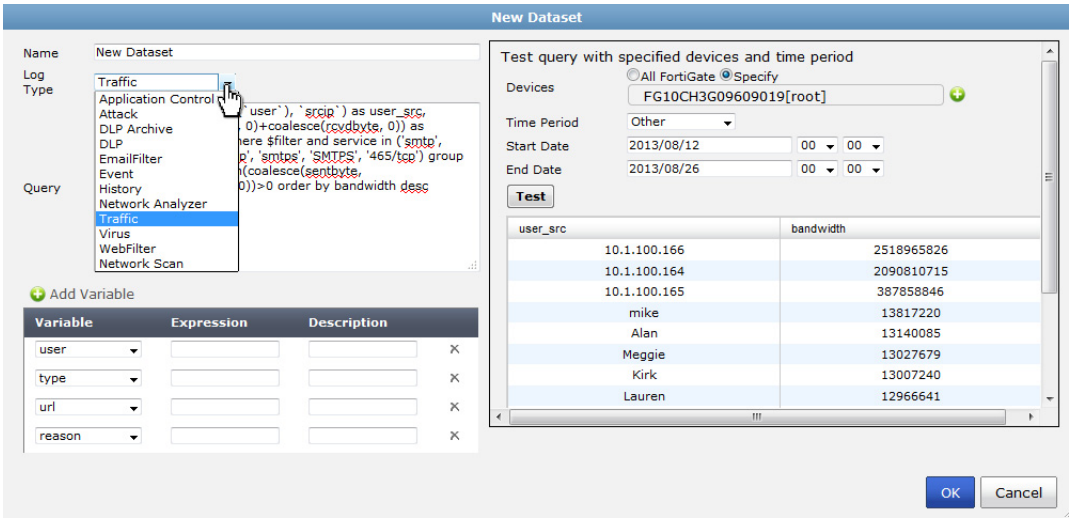
Create New	Select to create a new dataset. See “To create a new dataset:” on page 189.
Edit	Select to edit an existing dataset. See “To edit a dataset:” on page 190.
Delete	Select to delete a dataset. See “To delete datasets:” on page 190.
Clone	Select to clone an existing dataset. See “To clone a dataset:” on page 190.
Search	Use the search field to find a specific dataset.
Name	The name of the dataset.
Device Type	The device type that the dataset applies to.
Log Type	The type of log that the dataset applies to.
Page navigation	Adjust the number of logs that are listed per page and browse through the pages.

To create a new dataset:

1. In the dataset list, either select *Create New* from the toolbar, or right-click in the dataset list and select *Create New* from the pop-up menu.

   The *New Dataset* dialog box opens.

   Figure 140: Create a new dataset



2. Enter the required information for the new dataset.

Name	Enter a name for the dataset.
Log Type	Select a log type from the drop-down list. The following log types are available for FortiGate: *Application Control, Attack, DLP Archive, DLP, Email Filter, Event, Traffic, Virus, Web Filter,* and *Network Scan*. The following log types are available for FortiMail: *Email Filter, Event, History,* and *Virus*. The following log types are available for FortiWeb: *Attack, Event,* and *Traffic*.
Query	Enter the SQL query used for the dataset.
Add Variable	Select to add a variable, expression, and description information.
Test query with specified devices and time period	
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 list to select a time period. When selecting Other, enter the start date, time, end date, and time.
Test	Select Test to test the SQL query before saving the dataset configuration.

3. Test the query to ensure that the dataset functions as expected, then select *OK* to create the new dataset.

To clone a dataset:

1. In the dataset list, either select a dataset then select *Clone* from the toolbar, or right-click on the dataset then select *Clone* from the pop-up menu.

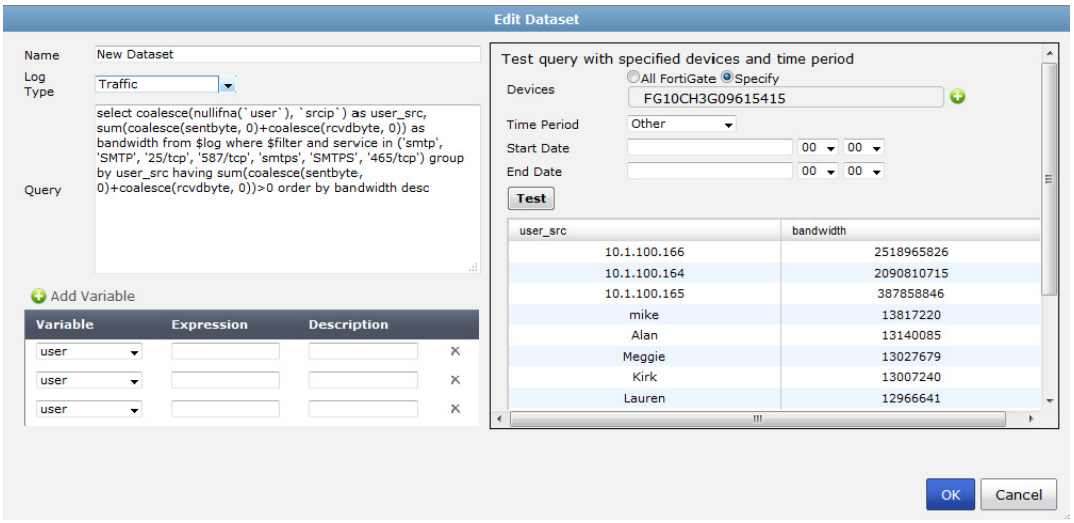
   The *Clone Dataset* dialog box opens.
2. Edit the information as required, then test the query to ensure that the dataset functions as expected.
3. Select *OK* to create a new, cloned dataset.

To edit a dataset:

1. In the dataset list double-click on the dataset, or select the dataset then select *Edit* from the toolbar or right-click menu.

   The *Edit Dataset* dialog box opens.

Figure 141: Edit a dataset



2. Edit the information as required, then test the query to ensure that the dataset functions as expected.
3. Select *OK* to finish editing the dataset.

Predefined datasets cannot be edited, the information is read-only. You can view the SQL query and variables used in the dataset and test against specific devices or log arrays.

To delete datasets:

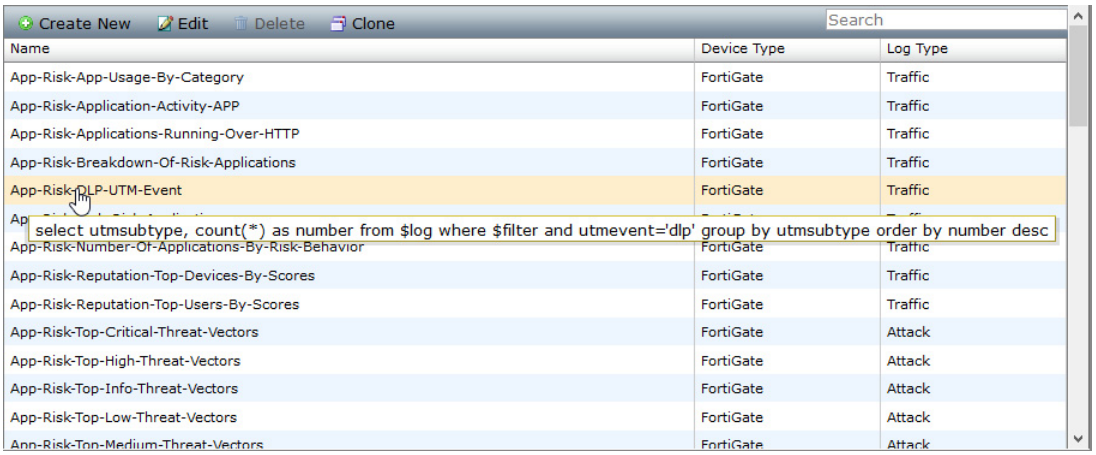
1. Select the dataset or datasets that you would like to delete, then select *Delete* from the toolbar or right-click menu.
2. Select *OK* in the confirmation dialog box to delete the selected datasets or datasets.

Predefined datasets cannot be deleted, the information is read-only.

To view the SQL query for an existing dataset:

Hover the mouse cursor over one of the datasets in the dataset list. The SQL query is displayed in a pop-up window.

Figure 142:SQL query pop-up window

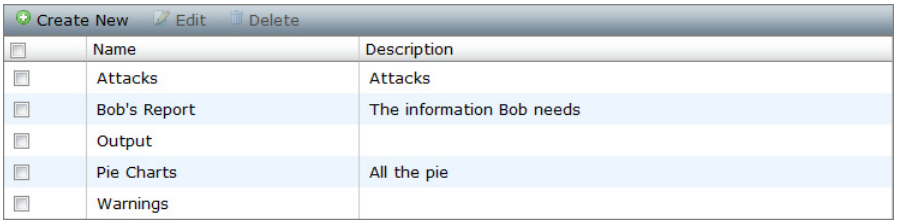


Output profile

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 for a report; see “Reports” on page 154.

To view and manage output profiles, go to *Reports* > *Advanced* > *Output Profile*.

Figure 143: Output profile page



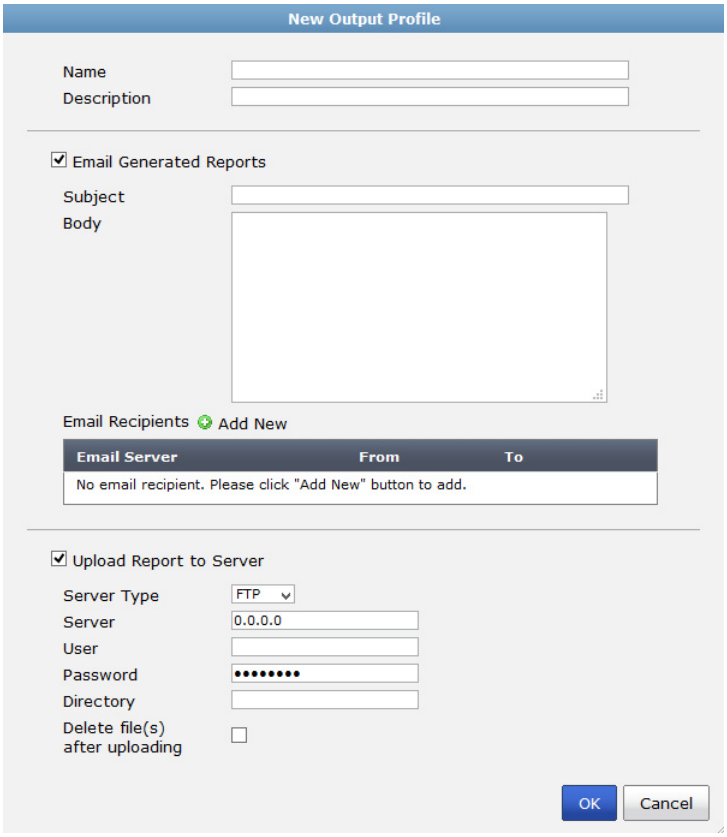
You must configure a mail server before you can configure an output profile. Please see “Mail server” on page 118 for information on configuring a mail server.

To create a new output profile:

1. In the output profile list, select *Create New* from either the toolbar or right-click menu.

   The *New Output Profile* dialog box opens.

Figure 144: Create new output profile dialog box



2. Enter the following information:

Name	Enter a name for the new output profile.
Description	Enter a description for the output profile (optional).
Email Generated Reports	Enable email generated reports.
Subject	Enter a subject for the report email.
Body	Enter body text for the report email.
Email Recipients	Select the email server from the drop-down list and enter to and from email addresses. Select *Add New* to add another entry so that you can specify multiple recipients.
Upload Report to Server	Enable uploading the reports to a server.
Server Type	Select *FTP*, *SFTP*, or *SCP* from the drop-down list.
Server	Enter the server IP address.
User	Enter the username.
Password	Enter the password.

Directory	Specify the directory where the report will be saved.
Delete file(s) after uploading	Select to delete the report after it has been uploaded to the selected.

3. Select *OK* to create the new output profile.

To edit an output profile:

1. In the output profile list, double-click on the output profile that you would like to edit, or select the output profile and select *Edit* from the toolbar or right-click menu.

   The *Edit Output Profile* dialog box opens.
2. Edit the information as required, then select *OK* to apply your changes.

To delete output profiles:

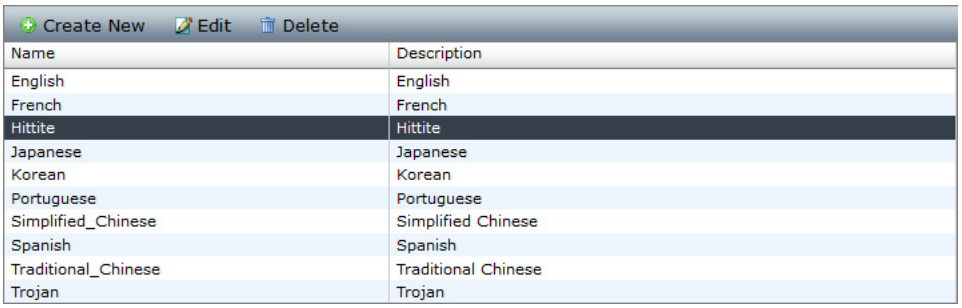
1. In the output profile list, select the output profile or profiles that you would like to delete, then select *Delete* from the toolbar or right-click menu.
2. Select *OK* in the confirmation dialog box to delete the selected output profile or profiles.

Language

The language of the reports can be specified when creating a report (see "Language & print options" on page 164). New languages can be added, and the name and description of the languages can be changed. The predefined languages cannot be edited.

To be viewed and managed report languages, go to *Reports* > *Advanced* > *Language*.

Figure 145: Report language



The available, pre-configured report languages include:

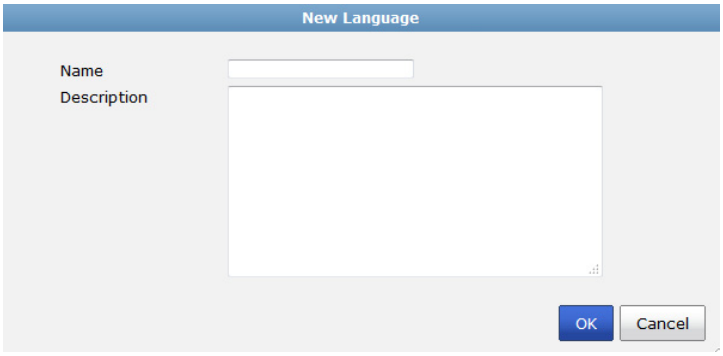
- English (default report language)
- French
- Japanese
- Korean
- Portuguese
- Simplified Chinese
- Spanish
- Traditional Chinese

To add a language:

1. In the report language list, select *Create New* from the toolbar or right-click menu.

   The *New Language* dialog box opens.

   Figure 146: Create a new language



2. Enter a name and description for the language in the requisite fields.
3. Select *OK* to add the language.

Adding a new language does not create that language. It only adds a placeholder for that language that contains the language name and description.

To edit a language:

1. In the report language list, double-click on the language that you would like to edit, or select the language and select *Edit* from the toolbar or right-click menu.

   The *Edit Language* dialog box opens.
2. Edit the information as required, then select *OK* to apply your changes.

Predefined languages cannot be edited; the information is read-only.

To delete languages:

1. In the report language list, select the language or languages that you would like to delete and select *Delete* from the toolbar or right-click menu.
2. Select *OK* in the confirmation dialog box to delete the selected language or languages.

Predefined languages cannot be deleted; the information is read-only.

FortiAnalyzer Firmware

This section explains how to properly upgrade to FortiAnalyzer v5.0 Patch Release 6. The following topics are included in this sections:

- Upgrading from FortiAnalyzer v5.0 Patch Release 5
- Upgrading from FortiAnalyzer v4.0 MR3
- General firmware upgrade steps
- Downgrading to previous versions

For detailed instructions on upgrading your FortiAnalyzer device, refer to the *FortiAnalyzer Release Notes* and *FortiAnalyzer Upgrade Guide*.

Read the release notes before upgrading your device.

Upgrading from FortiAnalyzer v5.0 Patch Release 5

FortiAnalyzer v5.0 Patch Release 6 officially supports upgrade from FortiAnalyzer v5.0 Patch Release 5.

Upgrading from FortiAnalyzer v4.0 MR3

FortiAnalyzer v5.0 Patch Release 6 officially supports upgrade from FortiAnalyzer v4.0 MR3 Patch Release 7.

Upon upgrading to FortiAnalyzer v5.0 Patch Release 1, your v4.0 MR3 logs are automatically converted and inserted into the SQL database. An icon appears at the top right corner after login to the Web-based Manager next to the logout and help buttons. This pops-up a small window displaying the progress.

In FortiAnalyzer v4.0 MR3, the Open Virtualization Format (OVF) setting uses 2 virtual CPUs, however v5.0 uses 1 virtual CPU. It is essential to change the vCPU setting to 1 before upgrading your FortiAnalyzer VM to avoid server instability or other serious issues.

Upgrade to the latest VMware ESXi 4.1 Patch Release (build 800380 or later) before upgrading FortiAnalyzer VM or changing the vCPU setting. If ESXi server instability or a purple diagnostic screen issue persists, please contact VMware support for proper guidance.

General firmware upgrade steps

The following table lists the general firmware upgrade steps.

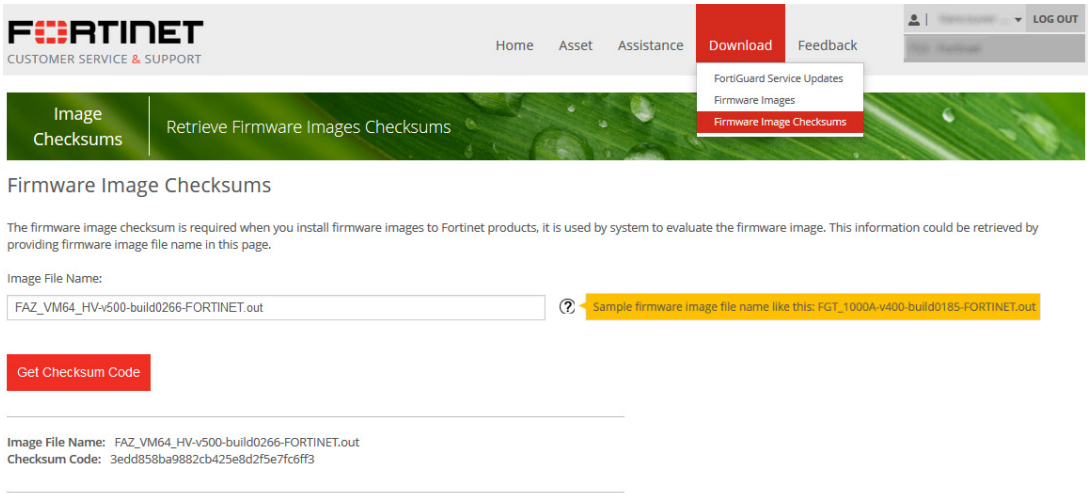
Table 8: Upgrade steps

Step 1	Prepare your FortiAnalyzer for upgrade.
Step 2	Backup your FortiAnalyzer system configuration. For FortiAnalyzer VM, take a *Snapshot* of the VM instance.
Step 3	Transfer the firmware image to your FortiAnalyzer device.
Step 4	Log into your FortiAnalyzer Web-based Manager to verify the upgrade was successful.

Step 1: Prepare your FortiAnalyzer for upgrade

1. Make sure all log devices are running the supported firmware version as stated in the release notes.
2. To verify the integrity of the download, go back to the *Download* section of the Customer Service & Support portal, then select the *Firmware Image Checksums* link. Optionally, you can select *Download* from the toolbar and select *Firmware Image Checksums* from the drop-down list.

Figure 147: Firmware image checksums page



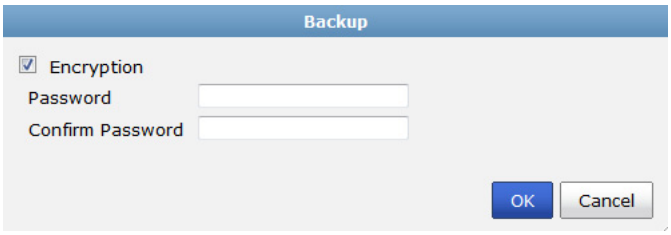
3. Enter the file name and select *Get Checksum Code* to get the firmware image checksum code. Compare this checksum with the checksum of the firmware image.

Step 2: Back up your FortiAnalyzer configuration

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

   The *Backup* dialog box opens.

   Figure 148: 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 FortiAnalyzer device.

4. Select *OK* and save the backup file on your local computer.

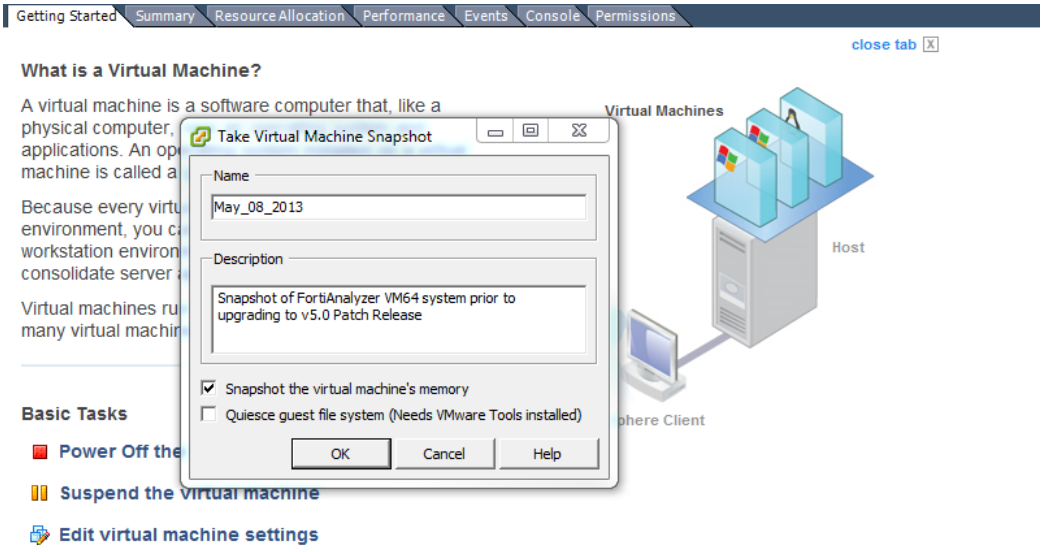
The system configuration file from a FortiAnalyzer v4.0 MR3 device cannot be directly imported into a FortiAnalyzer v5.0 Patch Release 6 device.

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} <server IP address>
     <path/filename to the server> <user name on server> <password>
     [cryptpasswd]
execute backup all-settings scp <server IP address> <path/filename to
     the server> <user name on server> <SSH certificate> <crptpassrd>
```

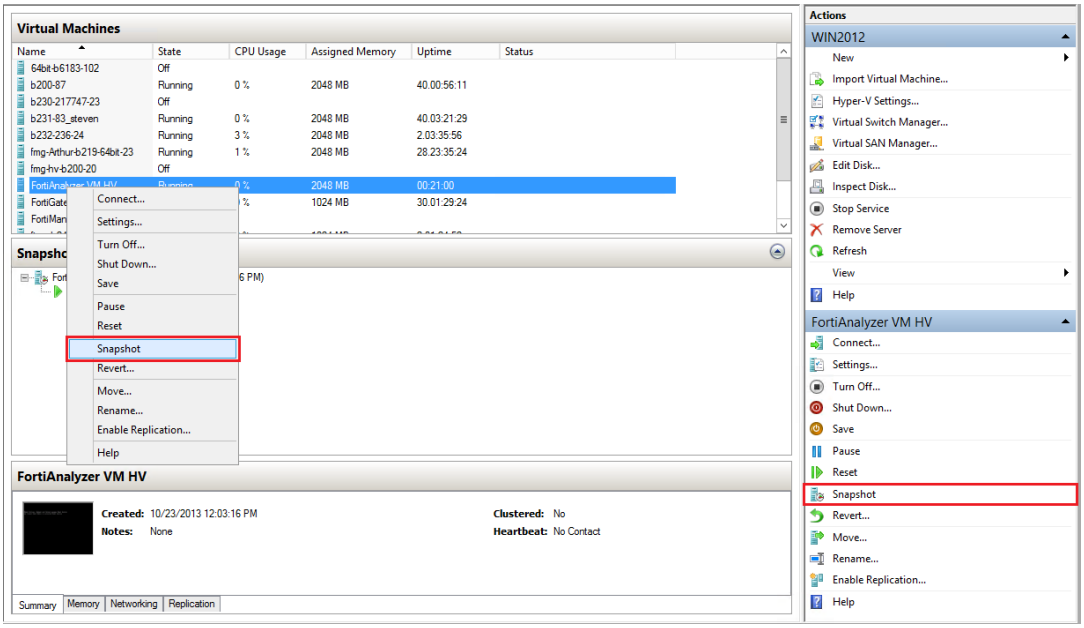
5. In VM environments, it is recommended that you take a *Snapshot* of the VM instance. In the event of an issue with the firmware upgrade, use the *Snapshot Manager* to revert to the *Snapshot*. To create a *Snapshot*, right-click the VM instance and select *Snapshot* > *Take Snapshot*.

Figure 149: Snapshot of FortiAnalyzer VM (VMware)



For information on snapshots in Microsoft Hyper-V Server environments, refer to the Microsoft Windows Server online help.

Figure 150: Snapshot of FortiAnalyzer VM (Microsoft Hyper-V)



Step 3: Transfer the firmware image to your FortiAnalyzer device

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Firmware Version* field, select *Update*.

   The *Firmware Upgrade* dialog box opens.
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 FortiAnalyzer will upload the firmware image and you will receive the following message: *The firmware upload is complete. The upgrade process has begun. Please refresh your browser in a few minutes*.

Optionally, you can upgrade firmware stored on a FTP or TFTP server using the following CLI command:

```
exexute restore image {ftp | tftp} <file path on the FTP server>
     <server IP address <user name on server> <password>
```

Step 4: Verify the upgrade

1. Refresh the browser page and log back in to the device.
2. In the *Device Manager* tab, ensure that all formerly added log devices are still listed.
3. Launch other functional modules to ensure that they work properly.

Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous FortiAnalyzer 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, and the hard drives might be formatted automatically.

Firmware downgrade is not recommended as it could lead to log data loss.

To re-initialize a FortiAnalyzer, use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```

Appendix A: SNMP MIB Support

The FortiAnalyzer SNMP agent supports the following MIBs:

Table 9: FortiAnalyzer MIBs

MIB or RFC	Description
FORTINET-CORE-MIB	This Fortinet-proprietary MIB enables your SNMP manager to query for system information and to receive traps that are common to multiple Fortinet devices.
FORTINET-FORTIMANAGER-FORTIANALYZER-MIB	This Fortinet-proprietary MIB enables your SNMP manager to query for FortiAnalyzer-specific information and to receive FortiAnalyzer-specific traps.
RFC-1213 (MIB II)	The FortiAnalyzer SNMP agent supports MIB II groups, except: • There is no support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). • Protocol statistics returned for MIB II groups (IP, ICMP, TCP, UDP, etc.) do not accurately capture all FortiAnalyzer traffic activity. More accurate information can be obtained from the information reported by the FortiAnalyzer MIB.
RFC-2665 (Ethernet-like MIB)	The FortiAnalyzer SNMP agent supports Ethernet-like MIB information except the dot3Tests and dot3Errors groups.

You can obtain these MIB files from the Customer Service & Support portal: https://support.fortinet.com.

To be able to communicate with your FortiAnalyzer unit's SNMP agent, you must first compile these MIBs into your SNMP manager. If the standard MIBs used by the SNMP agent are already compiled into your SNMP manager, you do not have to compile them again.

To view a trap or query's name, object identifier (OID), and description, open its MIB file in a plain text editor.

All traps that are sent include the message, the FortiAnalyzer unit's serial number, and the host name.

For instructions on how to configure traps and queries, see "Configuring the SNMP agent" on page 114.

Appendix B: Port Numbers

The following tables describe the port numbers that the FortiAnalyzer unit uses:

- ports for traffic originating from units (outbound ports)
- ports for traffic receivable by units (listening ports)
- ports used to connect to the FDN.

Traffic varies by enabled options and configured ports. Only default ports are listed.

Table 10: FortiAnalyzer outbound ports

Functionality	Port(s)
DNS lookup	UDP 53
NTP synchronization	UDP 123
Windows share	UDP 137-138
SNMP traps	UDP 162
Syslog, log forwarding	UDP 514 ***Note:*** If a secure connection has been configured between a FortiGate device and a FortiAnalyzer device, syslog traffic will be sent into an IPsec tunnel. Data will be exchanged over UDP 500/4500, Protocol IP/50.
Log and report upload	TCP 21 or TCP 22
SMTP alert email	TCP 25
User name LDAP queries for reports	TCP 389 or TCP 636
RADIUS authentication	TCP 1812
TACACS+ authentication	TCP 49
Log aggregation client	TCP 3000
Device registration of FortiGate or FortiManager units; remote access to quarantine, logs and reports from a FortiGate unit; remote management from a FortiManager unit (configuration retrieval) (OFTP)	TCP 514

Table 11: FortiAnalyzer listening ports

Functionality	Port(s)
Windows share	UDP 137-139 and TCP 445
Syslog, log forwarding	UDP 514 Note: If a secure connection has been configured between a FortiGate and a FortiAnalyzer, syslog traffic will be sent into an IPsec tunnel. Data will be exchanged over UDP 500/4500, Protocol IP/50.
SSH administrative access to the CLI	TCP 22
Telnet administrative access to the CLI	TCP 23
HTTP administrative access to the Web-based Manager	TCP 80
HTTPS administrative access to the Web-based Manager; remote management from a FortiManager unit	TCP 443
Device registration of FortiGate or FortiManager units; remote access to quarantine, logs and reports from a FortiGate unit; remote management from a FortiManager unit (configuration retrieval) (OFTP)	TCP 514
NFS share	TCP 2049
HTTP or HTTPS administrative access to the Web-based Manager's CLI dashboard widget. Protocol used will match the protocol used by the administrator when logging in to the Web-based Manager.	TCP 2032
Log aggregation server Log aggregation server support requires model FortiAnalyzer 800 series or greater.	TCP 3000
Remote management from a FortiManager unit (configuration installation)	TCP 8080
Remote MySQL database connection	TCP 3306

Appendix C: Maximum Values Matrix

Maximum values matrix

Table 12 lists maximum values per FortiAnalyzer model.

Table 12: Maximum values of FortiAnalyzer models

Feature	FAZ-100C, FAZ-200D	FAZ-300D, FAZ-400B, FAZ-400C	FAZ-1000B, FAZ-1000C FAZ-1000D	FAZ-2000A, FAZ-2000B	FAZ-3000D, FAZ-4000A, FAZ-4000B	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100
Administrative Domains (ADOMS)	100, 150	175, 200, 300	2000	2000	2000	10000	10000	10000	10000	10000
Administrators	256	256	256	256	256	256	256	256	256	256
Administrator access profiles	256	256	256	256	256	256	256	256	256	256
SNMP community	256	256	256	256	256	256	256	256	256	256
SNMP managers per community	256	256	256	256	256	256	256	256	256	256
Email servers	256	256	256	256	256	256	256	256	256	256
Syslog servers	256	256	256	256	256	256	256	256	256	256
TACACS+ servers	256	256	256	256	256	256	256	256	256	256
Administrator RADIUS servers	256	256	256	256	256	256	256	256	256	256
Administrator LDAP servers	256	256	256	256	256	256	256	256	256	256
Static routes	256	256	256	256	256	256	256	256	256	256
Log devices	100, 150	175, 200, 300	2000	2000	2000	10000	10000	10000	10000	10000
Devices per ADOM	100, 150	175, 200, 300	2000	2000	2000	10000	10000	10000	10000	10000

Table 12: Maximum values of FortiAnalyzer models (continued)

Log arrays	100, 150	175, 200, 300	2000	2000	2000	10000	10000	10000	10000	10000
Report output profiles	250	250	500	750	1000	1000	1000	1000	1000	1000
SQL report templates	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
SQL report charts	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
SQL report datasets	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
SQL database size (GB)	1000	4000, 1000, 2000	1000, 8000	3K, 12K	16K, 6K, 24K	200	+200	+1000	+8K	+16K

Appendix D: FortiAnalyzer VM

Licensing

Fortinet offers the FortiAnalyzer VM in a stackable license model based on GB logs per day and storage add-ons. This model allows you to expand your VM solution as your environment expands. When configuring your FortiAnalyzer, ensure that you configure the hardware settings as outlined in Table 13 and consider future expansion.

Table 13: FortiAnalyzer VM license information

Technical Specification	VM-Base	VM-GB1	VM-GB5	VM-GB25	VM-GB100
Hypervisor Support	VMware ESX versions 4.0 and 4.1 VMware ESXi versions 4.0, 4.1, 5.0, 5.1, and 5.5 Microsoft Hyper-V Server 2008 R2 and 2012				
VM Form Factor	VMware ESX/ESXi: Open Virtualization Format (OVF) Microsoft Hyper-V Server: Virtual Hard Disk (VHD)				
Devices / ADOMs Supported	10,000				
Virtual CPUs (Minimum / Maximum)	1 / Unlimited				
Virtual Network Interfaces (Minimum / Maximum)	1 / 4				
Virtual Memory (Minimum / Maximum)	2GB / Unlimited The default memory size is 2GB				
Virtual Storage (Minimum)	40GB				
Device Quota	200GB	+200GB	+1TB	+8TB	+16TB
Sessions / Day	3.5 M	3.5 M	18 M	85 M	360 M

For more information see the FortiAnalyzer product datasheet available on the Fortinet web site, http://www.fortinet.com/products/fortianalyzer/index.html.

FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer 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 FortiAnalyzer VM installation.
- `.ovf.zip`: Download either the 32-bit or 64-bit package for a new FortiAnalyzer 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.

Microsoft Hyper-V Server

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

Appendix E: MySQL databases

Setting up FortiAnalyzer with an external MySQL database

Follow the steps listed below to setup your FortiAnalyzer with an external MySQL database.

Set up your MySQL server:

1. Validate that you have a supported version of MySQL. This information will be displayed when you first log into the MySQL monitor. FortiAnalyzer v5.0 Patch Release 6 supports MySQL Server v5.5.
2. Set your server to bind to an accessible address and restart the server. This can be the IP address of any interface on the database host. Fortinet recommends using a private network or a direct cross-connection. Locate the `my.cnf` file associated with your MySQL installation and change the `bind-address` to the appropriate IP address.
3. Restart the server.
4. Create a user for your FortiAnalyzer device to use. You will need to create a user with privileges to create a database schema, create tables, update, insert, and select. You can edit these privileges after you have picked a schema name.

The minimum privileges for your external FortiAnalyzer user should include SELECT, INSERT, UPDATE, DELETE, EXECUTE, CREATE, ALTER, INDEX, and DROP.

Set up your FortiAnalyzer device:

1. In the FortiAnalyzer CLI console, enter the SQL configuration area:
   ```
   config system sql
   ```
2. Set the SQL status as remote:
   ```
   set status remote
   ```
3. Set the user name and password of the external user you have configured on your MySQL Server:
   ```
   set username <username_string>
   set password <password_string>
   ```
4. Set the database name:
   ```
   set database-name <database_name_string>
   ```
   Note that whatever name you enter here will create two schemas on your database server, one called ***.db and the other called ***_hcache.db.
5. Tell the FortiAnalyzer how to connect to the server with the following commands:
   ```
   set database-type mysql
   set server <server_IP_address>
   ```
6. Exit the `config system sql` menu using the end command:
   ```
   end
   ```

7. You can validate the connection to your remote database one of two ways: connect to the database server and check for your new schemas, or turn on SQL plugin debugging on your FortiAnalyzer unit and enter the following CLI command:

```
diagnose debug application sqlplugind 8
```

This command will allow you to see if a connection has occurred.

Index

A

access
  administrative 35
  change 35
  console 71
acknowledge
  events 128, 130
add
  break 175
  chart 174
  chart filter 175
  hard disk 83
  headings 171
  image 173
  language 194
  log array 52
  model device 45
  section 169
  static route 87, 88
  text box 172
administrative domain. See ADOM
administrator
  access 35
  accounts 89, 92
  configure 91
  create new 92
  current 61
  delete 90, 94
  disconnect 90
  edit 94
  monitor 90
  netmask 93
  profiles 95
  sessions 90
  settings 104
  timeout 90
  trusted host 95
ADOM 75
  administrators 41, 42
  advanced mode 42
  assign devices 41
  create new 39, 76
  delete 41, 77
  device modes 42
  disable 38, 77
  edit 40, 76
  enable 38, 61
  FortiMail 38
  FortiWeb 38
  mode 123
  name 39, 40
alert
  console 70
  email events 135
  logs 134
  mail server 118
  messages 70
analyzer mode 26, 27, 28
antivirus
  events 131
  logs 137
API 123
archive
  logs 145
ASCII 62
assign
  devices 41
authentication
  remote 99
automatic
  delete 122

B

backup 64
  configuration 61
  encrypt 64, 197
  logs 22
  password 64, 65
  reports 22
  restore 65
bookmark 143
  delete 143
browse
  log 146

C

CA
  certificate 108
  download 109
  import 108
  issuing 109
  view 108
calendar 186
certificate revocation list. See CRL
certificates 105
  CA 108
  delete 107, 109
  download 107, 109
  import 106, 108
  local 105, 106
  request 105
  view 106, 108

change
access 35
date 62
host name 62
language 34, 193
mode 54, 65
time 62
characters
special 62
chart 174
add 174
add filter 175
category 183
clone 184
create new 178, 183
custom 179
dataset 183
delete 185
edit 175, 185
filters 180
manage 183
name 183
predefined 178
type 182
wizard 178, 179
CLI 13, 71
commands 58, 71
console 58, 71
widget 57
clock 63
clone
chart 184
dataset 190
event handler 136
report 162
collector mode 26, 27, 28, 54
column
log view 141
order 141
settings 44
comma seperated value. See CSV
command line interface. See CLI
command prompt 61, 71
community
name 116
SNMP 115
configuration
backup 61, 64
restore 65
configure 166
administration 104
administrator 91, 98
backup 61
date 62
events 20, 127
interfaces 86
log forwarding 54
mail server 118
profiles 98
RAID 78
report templates 166
routing 87, 88
SNMP 114
syslog server 118
time 62
connect
secure 50
Web-based Manager 32
console
access 71, 95
CPU
usage 68
create new
administrator 92
ADOM 39, 76
certificate request 105
chart 178, 183
dataset 189
event handler 134
language 194
LDAP server 101
metadata field 120
output profile 191
profile 98
RADIUS server 102
report 161
report folder 162
route 87, 88
SNMP community 116
TACACS+ server 103
CRL 109
import 109
view 109
CSV 110, 144, 149
custom
charts 179
columns 140
dashboard 59
log view 139
profile 98
resource information 69
timeframe 142

D

daily
log rolling 151

dashboard
add widget 59
alert message console 70
CLI console 71
customize 59
data received 72
license information 66
log receive monitor 73
logs received 72
options 59
RAID monitor 77
reset 59
statistics 72
system information 60
system resources 68
unit operation 67
data
drill down 125, 126
email activity 125
threat activity 126
traffic activity 124
web activity 125
widget 72
database 14, 26
build 51
logs 37
rebuild 51
SQL 29
dataset
chart 183
clone 190
create new 189
delete 190
edit 190
report 187
SQL query 189, 191
date
configure 62
set 63
daylight saving 63
default
gateway 84
password 13
reports 156
settings 37
delete
administrator 90, 94
ADOM 41, 77
automatic 122
certificate 107, 109
charts 185
datasets 190
device 50
element 170
event handler 136
languages 194
log array 54
metadata field 120
output profiles 193
profile 99
report 54, 165
report folder 162
report template 162
schedule 187
search 143
server 100
SNMP community 117
SNMP manager 116
task 112
VDOM 50
device
add model 45
assign 41
delete 50
edit 49
logs 150
modes 42
reports 54, 166
diagnostic tools 89
disable
ADOMs 38, 77
event handler 136
log rolling 151
log uploads 150
schedule 186
DLP
events 132
DNS
port 201
servers 84
download
certificate 107, 109
log file 149
reports 54, 165, 187
WSDL file 123
drill down 19
data 125, 126
email activity 125
threat activity 126
traffic activity 124
web activity 125

E

edit
- administrator 94
- ADOM 40, 76
- chart 175, 185
- cover page 176
- dataset 190
- device 49
- event handler 136
- headings 171
- image 174
- language 194
- log array 53
- metadata field 120
- output profile 193
- schedule 186
- section 169
- SNMP community 117
- text box 172
- workspace 167

electrostatic discharge. See ESD

element
- break 175
- chart 174
- delete 170
- footer 170
- heading 171
- image 173
- move 170
- text box 172

email activity
- drill down 125
- view data 125

enable
- ADOMs 38, 61
- event handler 136
- log uploads 150
- SNMP agent 114
- SNMP query 117
- SNMP traps 117

encrypt
- backup 64, 197

ESD 82

event handler 131
- clone 136
- create new 134
- delete 136
- disable 136
- DLP 132
- edit 136
- enable 136
- filters 133
- log alerts 134
- name 133
- severity 133
- traffic logs 134

event management
- SNMP trap 136
- syslog server 136

events
- acknowledge 128, 129, 130
- alert email 135
- antivirus 131
- category 135
- configure 20, 127
- details 129
- log 129, 134
- management 20, 127
- monitor 127
- print 129
- raw logs 129
- review notes 129
- severity 128
- SNMP 117, 136

export
- certificates 105
- log files 137
- report template 176
- reports 20

F

FDN
- ports 201

filter
- chart 175, 180
- events 133
- log type 135
- logs 141
- report 164

firmware 60
- update 63

FortiAnalyzer
- maximum values 203
- ports 201
- RAID levels 81
- reboot 37
- shutdown 37
- upgrade 195
- VM 20, 203

FortiClient
- logging 22, 149
- support 22

FortiMail 19
- ADOMs 38

FortiWeb 19
- ADOMs 38

FQDN 119

FTP server 121

H

HA 50, 51, 85, 137

hard disk
- add 83
- hot-swapping 82
- usage 69

headings 171

high availability. See HA

host
name 60, 61, 62
trusted 36, 95
hot swap 82

I

idle timeout 36, 104
image 173
import
certificate 108
CRL 109
local certificate 106
log file 148
report template 176
reports 20
information
customize 69
installation 13
interface 85
configure 86
list 85, 86
management 84
IPS
events 132

J

javascript 71

L

language 105
add 194
change 34
delete 194
edit 194
report 164, 193
Web-based Manager 34
LDAP server
configuration 101
create new 101
delete 100
modify 100
ports 201
license
information 66
upload 67
VM 67
lightweight directory access protocol. See LDAP
list
interfaces 85, 86
size 123
log
archive 145
backup 22
browse 146
download 149
events 134
FortiClient 149
forwarding 54
import 148
messages 110
ports 201
raw 129
receive monitor 73
reliability 22
reset 37
restore 22
rolling 151, 152
rotation 121
search 142
settings 113, 121
storage 29
traffic 134
type 180
type filters 135
upload 121, 150
view 110, 137
view packets 145
volume 28
widget 72
log array 51
add 52
delete 54
edit 53
rebuild 53
rebuild database 51
log view 137
bookmark 143
columns 141
customize 139
details 145
favorite 143
filter 141
formatted 139
historical 139
raw 139
real time 139
search 142
timeframe 142
log_message_bookmarks 143

M

mail server 191
alerts 118
settings 118
manage
charts 183
events 20, 127
reports 54
management information base. See MIB
management interface 84

manager
connect to 32
mandatory 119
maximum values 203
memory
usage 69
metadata 119
add field 120
delete 120
edit 120
metafields 119
MIB 113, 114, 200
files 200
Fortinet 113, 200
mode 26
ADOM 123
advanced 42, 123
analyzer 27, 28, 29
change 54, 65
collector 27, 28, 29, 54
device 42
normal 123
modify
profile 99
server 100
monitor
administrators 90
events 127
logs 73
task 112

N

name
ADOM 39, 40
certificate 107, 108
chart 183
common 106
event handler 133
host 60, 61
report template 154
SNMP community 116
syslog server 119
netmask
administrator 93
network
diagnostic tools 85
interfaces 85, 86
management interface 84
routing table 85
settings 84
static routing 87, 88
traffic 134
network time protocol. See NTP
NTP 63
port 201

O

obfuscate 164
OFTP 50
operation mode 27

P

packet log 145
password 64, 65
administrator 13
policy 105
port
numbers 201
remote 117
status 67
print
events 129
profile
administrator 95
configure 98
create new 98, 191
delete 99, 193
edit 193
modify 99
report 165, 191
restricted 95
standard 95
super 95

R

RADIUS server 102
configure 102
create new 102
delete 100
modify 100
port 201
RAID 77
configure 78
level 78
management 18
monitor 77
supported levels 79–81
reboot 67
FortiAnalyzer 37
rebuild
log array 53
redundant array of independent disks. See RAID
remote
authentication 99
port 117
remote authentication dial-in user. See RADIUS
rename
chart 182
event handler 136
report folder 162

report
advanced settings 164
backup 22
calendar 186
clone 162
completed 165
cover page 164, 176
create new 161
datasets 187
delete 54, 165
device 54, 166
device list 164
download 54, 165, 187
filters 164
folder 162
language 164, 193
name 166
obfuscate 164
output profile 165, 191
per-device 154
ports 201
pre-defined 17
restore 22
run 162
schedule 154, 163, 186
status 166
table of contents 164
templates 17, 153
type 154
view 54
report template 153, 154, 166
breaks 175
chart 174
default 156
delete 162
element 170
export 176
headings 171
image 173
import 176
name 154
schedule 154
sections 168
text 172
time period 154
type 154
workspace 167
reset
dashboard 59
default settings 37
FortiAnalyzer 37
logs 37
resolution 31
restart 67
restore
backup 65
configuration 65
logs 22
reports 22
system 65
roll logs 151
route
add 87, 88
configure 87, 88
static 87, 88
run
report 162

S

schedule
delete 187
disable 186
edit 186
reports 154, 163, 186
SCP server 121
screen resolution 31
search
delete 143
log messages 142
save 143
sections 168, 169
secure
connection 50
secure shell. See SSH
serial number 60
server
authentication 99
delete 100
DNS 84
FTP 121
LDAP 101
mail 118, 191
modify 100
name 119
NTP 63
RADIUS 102
remote 99
SCP 121
SFTP 121
SMTP 118
syslog 118
TACACS+ 103
session
monitor 90
settings
administrator 104
advanced 113, 123
columns 44
default 37
device log 113
log 121
log rotation 121
mail server 118
network 84
syslog server 118
severity
event handler 133
events 128
SFTP server 121
shutdown 37, 67
simple network management protocol. See SNMP

SMTP
port 201
server 118
SNMP 113
agent 114, 200
configure 114
enable 114
events 117, 136
fields 114
manager 113, 114, 200
port 201
query 117
system name 61
traps 114, 117
SNMP community 115
create new 116
delete 117
edit 117
name 116
special characters 62
SQL 29
dataset 23, 189
external 207
port 202
query 23, 189
SSH 71
port 202
SSL 62
static routes 87
statistics
widget 72
status
event handler 133
task 112
strings 14
structured query language. See SQL 29
supported
web browsers 31
syslog server
events 136
FQDN 119
name 119
port 201
settings 118
system
advanced settings 113
backup 64
clock 63
date 63
firmware 60, 63
name 61
options 104
resources 68
restore 65
time 60, 62, 63
widget 60

T

TACACS+ server 103
configure 103
create new 103
delete 100
modify 100
port 201
task
delete 112
list size 123
monitor 112
status 112
view 112
TCP 149
template
breaks 175
charts 174
cover page 176
delete 162
element 170
headings 171
image 173
report 153
sections 168
text 172
workspace 167
terminal access controller access-control system. See TACACS+
text 14
text box 172
threat activity
drill down 126
view data 126
time
completed 165
configure 62
frame 142
out 104
report template 154
set 63
system 60, 63
up 61
zone 63
timeout 36, 104
administrator 90
traffic
activity 124
drill down 124
events 134
ports 201
tree menu 33
trusted host 36
security 95
tunnel 50

U

unit operation 67
update
firmware 63

upgrade
FortiAnalyzer 195
upload
enable 121
logs 121, 150
VM license 67
uptime 61
utilization
CPU 68
hard disk 69
memory 69

V

VDOM
delete 50
view
certificate 106, 108
CRL 109
email activity 125
event logs 129
log messages 129
logs 110, 137
packet log 145
reports 54
SQL query 191
task 112
threat activity 126
traffic activity 124
web activity 125

W

web activity
drill down 125
view data 125
web browser
supported 31
web filter
events 132
web services description language. See WSDL
Web-based Manager 32
content pane 33
language 34
tab bar 33
tree menu 33
weekly
log rolling 152
widget 58
add 59
alert message console 70
CLI 57
CLI console 71
license information 66
log receive monitor 73
logs/data received 72
move 59
options 59
RAID monitor 77
resource information 69
statistics 72
system information 60
system resources 68
unit operation 67
wizard 17, 19, 45, 178, 179, 182
WSDL 24, 113, 123
file download 123