

# FortiAnalyzer - Administration Guide

VERSION 5.4.0

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



November 23, 2016

FortiAnalyzer 5.4.0 Administration Guide

05-540-279341-20161123

# TABLE OF CONTENTS

<b>Change Log</b>	<b>12</b>
<b>Introduction</b>	<b>13</b>
FortiAnalyzer documentation	13
<b>What's New in FortiAnalyzer</b>	<b>14</b>
FortiAnalyzer 5.4.0	14
New GUI	14
FortiView extensions	14
Report extensions	14
Log storage and disk management	15
Collector and analyzer mode updates	15
Fetching	15
FortiClient log management	15
Log forwarding extensions	16
Other device support	16
<b>Key Concepts</b>	<b>17</b>
Operation modes	17
Analyzer mode	17
Analyzer and collector mode	18
Feature comparison between analyzer and collector mode	19
Administrative domains	20
Log storage	20
SQL database	20
Compressed logs and indexed logs	20
Data policy and automatic deletion	21
Disk utilization for compressed and indexed logs	21
<b>Overview</b>	<b>22</b>
Configuring FortiAnalyzer	22
Configuring FortiAnalyzer units in collector and analyzer modes	22
FortiAnalyzer one - configuring collector mode	22
FortiAnalyzer two - configuring analyzer mode	23
Viewing analyzed log data	23
Cannot view the Settings pane	24
<b>FortiAnalyzer GUI</b>	<b>25</b>

Connecting to the GUI .....	25
GUI overview .....	25
Panes .....	27
Switching between ADOMs .....	28
Using the right-click menu .....	28
Restarting and shutting down .....	29
<b>Network .....</b>	<b>30</b>
About the network .....	30
Ports .....	30
Administrative access .....	30
Restrict administrator access with trusted hosts .....	30
Configuring the network .....	30
Configuring ports and administrator access .....	30
Adding a static route .....	31
Managing the network .....	31
Viewing network settings .....	31
Editing network settings .....	32
Changing administrative access .....	32
Disabling ports .....	32
Network references .....	32
Network pane .....	32
Create New Network Route pane .....	33
Edit System Interface pane .....	33
<b>RAID .....</b>	<b>35</b>
About RAID .....	35
Supported RAID levels .....	35
RAID support per FortiAnalyzer model .....	37
Configuring RAID .....	38
Managing RAID .....	38
Monitoring RAID status .....	39
Swapping hard disks .....	39
Adding new disks .....	40
RAID references .....	40
RAID Management pane .....	40
<b>Administrative Domains .....</b>	<b>42</b>
About ADOMs .....	42
How ADOMs affect the GUI .....	42
Default ADOMs .....	42
FortiClient support and ADOMs .....	43
Considerations for creating ADOMs .....	43
ADOM device modes and VDOM support .....	43
Configuring ADOMs .....	44

Enabling ADOMs .....	44
Enabling advanced ADOM device mode .....	44
Creating ADOMs .....	44
Assigning devices to ADOMs .....	45
Assigning administrators to ADOMs .....	45
Managing ADOMs .....	46
Viewing all ADOMs .....	46
Disabling advanced ADOM mode .....	46
Disabling ADOMs .....	47
ADOM references .....	47
All ADOMs pane .....	47
Create or Edit ADOM pane .....	47
<b>Administrator Accounts .....</b>	<b>50</b>
About administrator accounts .....	50
Administrator accounts .....	50
How ADOMs affect administrator access .....	50
Trusted hosts .....	50
Administrator profiles .....	51
Configuring administrator accounts .....	52
Managing administrator accounts .....	53
Viewing administrator accounts .....	53
Viewing administrators logged into the FortiAnalyzer unit .....	53
Disconnecting administrators from the FortiAnalyzer unit .....	54
Administrator profiles .....	54
Managing administrator profiles .....	54
Creating custom administrator profiles .....	54
Remote authentication servers .....	55
Managing remote authentication servers .....	55
Adding an LDAP server .....	55
Adding a RADIUS server .....	57
Adding a TACACS+ server .....	57
Two-factor authentication .....	58
Configuring FortiAuthenticator .....	58
Configuring FortiAnalyzer .....	61
Global administrator settings .....	62
Configuring global administrative settings .....	62
Changing the GUI language .....	63
Changing the idle timeout .....	64
Administrator account references .....	64
Create Administrator page .....	64
Create Administrator Profile page .....	65
Global Administrator Settings page .....	66

<b>Devices</b>	<b>67</b>
About devices	67
How ADOMs affect devices	67
FortiClient EMS devices	67
Unregistered devices	67
Adding devices	67
Adding devices using the wizard	68
Adding devices manually	69
Managing registered devices	69
Using the quick status bar	70
Displaying historical average log rates	70
Managing unregistered devices	71
Device references	71
Device Manager pane > quick status bar	71
Device Manager > Devices Total pane	72
Device Manager > Unregistered Devices pane	73
Add Device wizard	73
Edit Device pane	74
<b>Log and File Storage</b>	<b>76</b>
About log and file storage	76
How ADOMs affect log storage	76
FortiAnalyzer disk space allocation	76
Disk fullness and automatic log deletion	77
Automatic deletion of logs and files	77
FortiAnalyzer log files for storing logs	78
Log and file workflow	79
Configuring log storage	80
Configuring log storage settings	80
Editing log storage settings	81
Monitoring log storage capacity	82
Managing log storage settings	82
Configuring global log and file settings	83
Configuring global automatic deletion	83
Configuring rolling and uploading of logs	83
Configuring rolling and uploading of logs by using the CLI	85
Managing logs	87
Log storage references	88
Storage Info pane	88
Edit ADOM Storage Configuration dialog box	89
<b>Reports</b>	<b>91</b>
About reports	91
How ADOMs affect reports	91

Predefined reports, templates, charts, and macros .....	91
Logs used for reports .....	92
How charts and macros extract data from logs .....	92
How auto-cache works .....	92
Generating reports .....	93
Generating reports .....	93
Viewing completed reports .....	93
Enabling auto-cache .....	93
Scheduling reports .....	93
Creating reports .....	94
Creating reports from report templates .....	94
Creating reports by cloning and editing .....	94
Creating reports without using a template .....	95
Customizing report cover pages .....	95
Managing reports .....	97
Organizing reports into folders .....	97
Importing and exporting reports .....	98
Report template library .....	98
Creating report templates .....	98
Creating report templates by saving a report .....	99
Viewing sample reports for predefined report templates .....	99
Managing report templates .....	99
Chart library .....	100
Creating charts .....	100
Managing charts .....	103
Macro library .....	104
Creating macros .....	104
Managing macros .....	105
Datasets .....	105
Creating datasets .....	105
Viewing the SQL query for an existing dataset .....	106
Managing datasets .....	107
Output profiles .....	107
Creating output profiles .....	107
Managing output profiles .....	109
Report languages .....	109
Predefined report languages .....	109
Adding language placeholders .....	109
Managing report languages .....	110
Report calendar .....	110
Viewing all scheduled reports .....	110
Managing report schedules .....	111

Report references .....	111
List of report templates .....	111
Reports Settings tab .....	113
Reports Layouts tab .....	115
<b>Event Monitor .....</b>	<b>120</b>
About events .....	120
How ADOMs affect events .....	120
Predefined event handlers .....	120
Logs used for events .....	120
Event handlers .....	120
Enabling event handlers .....	121
Creating custom event handlers .....	121
Filtering event handlers by predefined and custom .....	122
Searching event handlers .....	122
Resetting predefined event handlers to factory defaults .....	122
Managing event handlers .....	123
Events .....	123
Viewing event summaries .....	124
Viewing event details .....	124
Acknowledging events .....	125
Event references .....	125
List of predefined event handlers .....	125
Create New Handler pane .....	128
<b>FortiView .....</b>	<b>131</b>
About FortiView .....	131
How ADOMs affect the FortiView pane .....	131
Logs used for FortiView .....	131
Description of FortiView .....	131
Using FortiView .....	133
Viewing FortiView summary page .....	133
Viewing FortiView summaries in tabular format .....	136
Viewing FortiView summaries in graphical format .....	136
Filtering FortiView summaries .....	137
Viewing a map of top countries .....	137
Viewing the threat map .....	138
Viewing related logs .....	138
Exporting summary views to PDF .....	138
Monitoring disk usage for devices .....	138
Viewing log storage statistics .....	138
Examples of using FortiView .....	139
Finding application and user information .....	139
Finding unsecured wireless access points .....	140



Analyzing and reporting on network traffic .....	140
<b>Log View .....</b>	<b>141</b>
About Log View .....	141
How ADOMs affect the Log View tab .....	141
Logs used for Log View .....	141
Log arrays in FortiAnalyzer 5.2.0 and later .....	141
Types of logs collected for each device .....	141
Log messages .....	143
Viewing the log message list of a specific log type .....	143
Viewing log message details .....	143
Customizing displayed columns .....	144
Filtering log messages .....	145
Viewing historical and real-time logs .....	146
Viewing raw and formatted logs .....	146
Custom views .....	146
Downloading log messages .....	147
Creating charts with Chart Builder .....	147
Log arrays .....	148
Creating log arrays .....	148
Managing log arrays .....	148
Log Browse .....	148
Browsing log files .....	149
Importing a log file .....	149
Downloading a log file .....	150
Log View references .....	150
Chart Builder dialog box .....	150
<b>System Settings .....</b>	<b>151</b>
System settings tree menu .....	151
System settings dashboard .....	152
Customizing the dashboard .....	154
Configuring operation modes .....	155
Viewing port status .....	155
Viewing CPU status .....	155
Viewing alert messages .....	155
Viewing the number of logs being received .....	156
Setting the date and time .....	156
Changing the host name .....	157
Accessing the CLI .....	158
Licenses and firmware .....	158
Viewing license information .....	158
Uploading a FortiAnalyzer VM license .....	158
Viewing and updating FortiAnalyzer firmware .....	159

Local Certificates .....	159
Managing local certificates .....	159
Creating local certificate requests .....	159
Importing local certificates .....	160
Viewing details of local certificates .....	161
CA Certificates .....	161
Importing CA certificates .....	161
Viewing CA certificate details .....	161
Downloading CA certificates .....	162
Deleting CA certificates .....	162
Certificate revocation lists .....	162
Importing a CRL .....	162
Viewing a CRL .....	163
Deleting a CRL .....	163
Log Forwarding .....	163
Modes .....	163
Overview of configuring aggregation mode .....	164
Overview of configuring combined mode .....	164
Enabling log forwarding .....	164
Defining the user name and password .....	164
Enabling aggregation on the interface .....	165
Enabling the log aggregation service .....	165
Configuring log forwarding profiles .....	165
Managing log forwarding .....	166
Create New Log Forwarding pane .....	166
Log fetcher management .....	167
Overview of fetching logs .....	168
Preparing to fetch logs .....	168
Configuring fetch server profiles .....	169
Configuring fetch client profiles .....	169
Sending requests to fetch logs .....	169
Approving or rejecting requests to fetch logs .....	170
Monitoring request sessions .....	170
Managing fetch profiles .....	170
Fetcher Management references .....	171
FortiAnalyzer event log .....	172
FortiAnalyzer task monitor .....	175
Viewing tasks performed for the FortiAnalyzer unit .....	175
Deleting tasks .....	176
Filtering the task view .....	176
Configuring the task list size .....	176
SNMP .....	177

Configuring an SNMP agent .....	177
Mail servers .....	185
Configuring a syslog server .....	185
Syslog servers .....	186
Configuring a syslog server .....	186
Meta fields .....	187
Managing metadata fields .....	187
Creating new meta fields .....	187
WSDL files .....	188
Downloading WSDL files .....	188
System configuration backups .....	188
Backing up the system configuration .....	188
Restoring the system configuration .....	189
<b>Appendix A - Port Numbers .....</b>	<b>190</b>
<b>Appendix B - Maximum Values Matrix .....</b>	<b>192</b>
<b>Appendix C - SNMP MIB Support .....</b>	<b>194</b>
SNMP MIB Files .....	194
FORTINET-CORE-MIB .....	194
FORTINET-FORTIMANAGER-FORTIANALYZER-MIB .....	203

## Change Log

Date	Change Description
2016-02-17	Initial release
2016-03-02	Added a note in the "Importing a log file" section.
2016-03-24	Clarified configuration of log forwarding.
2016-11-23	Updated "Disk utilization for compressed and indexed logs" section to clarify storage ratio example.

# 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.

## FortiAnalyzer documentation

The following FortiAnalyzer product documentation is available:

- *FortiAnalyzer Administration Guide*  
This document describes how to set up the FortiAnalyzer system and use it with supported Fortinet units.
- FortiAnalyzer device *QuickStart Guides*  
These documents are included with your FortiAnalyzer system package. Use this document to install and begin working with the FortiAnalyzer system and FortiAnalyzer GUI.
- *FortiAnalyzer Online Help*  
You can get online help from the FortiAnalyzer GUI. FortiAnalyzer online help contains detailed procedures for using the FortiAnalyzer GUI to configure and manage FortiGate units.
- *FortiAnalyzer CLI Reference*  
This document describes how to use the FortiAnalyzer Command Line Interface (CLI) and contains references for all FortiAnalyzer CLI commands.
- *FortiAnalyzer Release Notes*  
This document describes new features and enhancements in the FortiAnalyzer system for the release, and lists resolved and known issues. This document also defines supported features, languages, platforms and firmware versions.
- *FortiAnalyzer VM Install Guide*  
This document describes installing FortiAnalyzer VM in your virtual environments.

# What's New in FortiAnalyzer

This section provides a summary of the new features and enhancements in FortiAnalyzer.

## FortiAnalyzer 5.4.0

FortiAnalyzer 5.4.0 includes the following new features and enhancements.

### New GUI

The FortiAnalyzer GUI has a new look and simplified navigation. When ADOMs are enabled, you now select an ADOM when you log into FortiAnalyzer. After you log in, you can choose which pane to display by choosing one of the following options: *Device Manager*, *FortiView*, *Log View*, *Event Monitor*, *Reports*, and *System Settings*. You can use the banner at the top of the FortiAnalyzer GUI to switch between ADOMs and panes. See [GUI overview on page 25](#).

### FortiView extensions

FortiView includes new summary views as well as more graphical display options. You can also print summary views and detailed views to PDF.

New summary views:

- *FortiView > Summary*
- *FortiView > Summary > Threats*: Threat Map
- *FortiView > Summary > Traffic*: Policy Hit
- *FortiView > Summary > Application & Websites*: Top Browsing Users
- *FortiView > Summary > WiFi*:
  - Authorized APs
  - Authorized SSIDs
  - WiFi Clients
- *FortiView > Summary > System*:
  - Storage Statistics
  - Failed Authentication Attempt
- *FortiView > Summary > Endpoints*: All FortiClient endpoints registered to FortiGates

See [FortiView on page 131](#).

### Report extensions

FortiAnalyzer includes the new reports, report templates, and charts. See [Reports on page 91](#).

New reports:

- Wireless PCI Compliance
- PCI DSS Compliance Review

- FortiSandbox Default Report
- FortiDDoS Default Report

New report templates:

- Template - 360 Security Review

New charts:

- Data loss prevention (DLP)
- Top 20 users by website browsing time

A new chart builder is also available on the *Log View* pane to help you build charts based on the logs that you are viewing. See [Creating charts with Chart Builder on page 147](#).

## Log storage and disk management

It is now easier to configure and monitor how much FortiAnalyzer disk space to use for log storage. You can now specify how long to keep logs online and indexed in the SQL database to support data analysis on the *Log View*, *FortiView*, and *Reports* tabs. You can also specify how long to store logs on the FortiAnalyzer unit in an offline, compressed format to support archiving. You can then monitor how quickly the allotted space is being consumed by logs. See [Log storage on page 20](#).

## Collector and analyzer mode updates

When the FortiAnalyzer unit is operating in collector mode, the SQL database is now disabled by default. Collector mode is useful for receiving and storing many logs from many managed devices. While in collector mode, logs are stored in a compressed format and can be stored for a longer period of time to support archiving, compliance requirements, and log search. You can control how long compressed logs are stored on the FortiAnalyzer unit by using a data policy.

You can then forward only the logs that you want to analyze to a FortiAnalyzer unit that is operating in analyzer mode. In analyzer mode, the SQL database is enabled by default, and logs are automatically indexed in the database to support data analysis on the *Log View*, *FortiView*, and *Reports* tabs. You may need only a short amount of time to analyze logs, and you can control how long logs are indexed in the database by using a data policy.

For more information, see [Operation modes on page 17](#), [Compressed logs and indexed logs on page 20](#), and [Log storage on page 20](#).

## Fetching

You can fetch offline, compressed logs from one FortiAnalyzer unit to a second FortiAnalyzer unit where the logs can be automatically indexed in the database to support data analysis on the *Log View*, *FortiView*, and *Reports* tabs. The fetch feature allows you to analyze data from compressed logs without affecting the performance of the primary FortiAnalyzer unit because the process of fetching logs happens in the background. See [Log fetcher management on page 167](#).

## FortiClient log management

You can now view and analyze logs from FortiClient endpoints that are registered to FortiGate devices or FortiClient EMS devices. You can view FortiClient logs under the device to which the endpoints are registered.

For example, you can view logs for FortiClient endpoints that are registered to a FortiGate device by viewing the FortiGate device. Alternately, you can view logs for FortiClient endpoints that are registered to a FortiClient EMS device by viewing the FortiClient EMS device. ADOMs must be enabled to support FortiClient EMS devices.

## Log forwarding extensions

You can now configure FortiAnalyzer to forward only the log messages that meet the requirements of specified filters. See [Log Forwarding on page 163](#).

## Other device support

FortiAnalyzer now supports FortiDDoS devices and FortiClient EMS servers.



# 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.

## Operation modes

The FortiAnalyzer unit has two operation modes:

- **Analyzer:** The default mode that supports all FortiAnalyzer features. This mode is 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* pane are disabled.

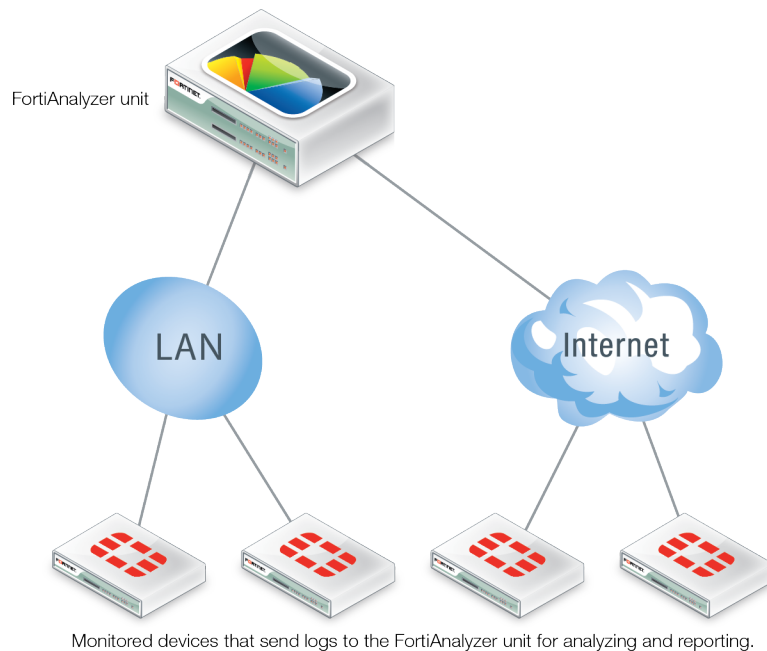
The analyzer and collector modes are used together to increase the analyzer's performance. The collector provides a buffer to the FortiAnalyzer by off-loading the log receiving task from the analyzer. Since log collection from the connected devices is the dedicated task of the collector, its log receiving 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 [Configuring operation modes on page 155](#).

## 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.

The topology of the unit in analyzer mode illustrates the network topology of the FortiAnalyzer unit in analyzer mode.

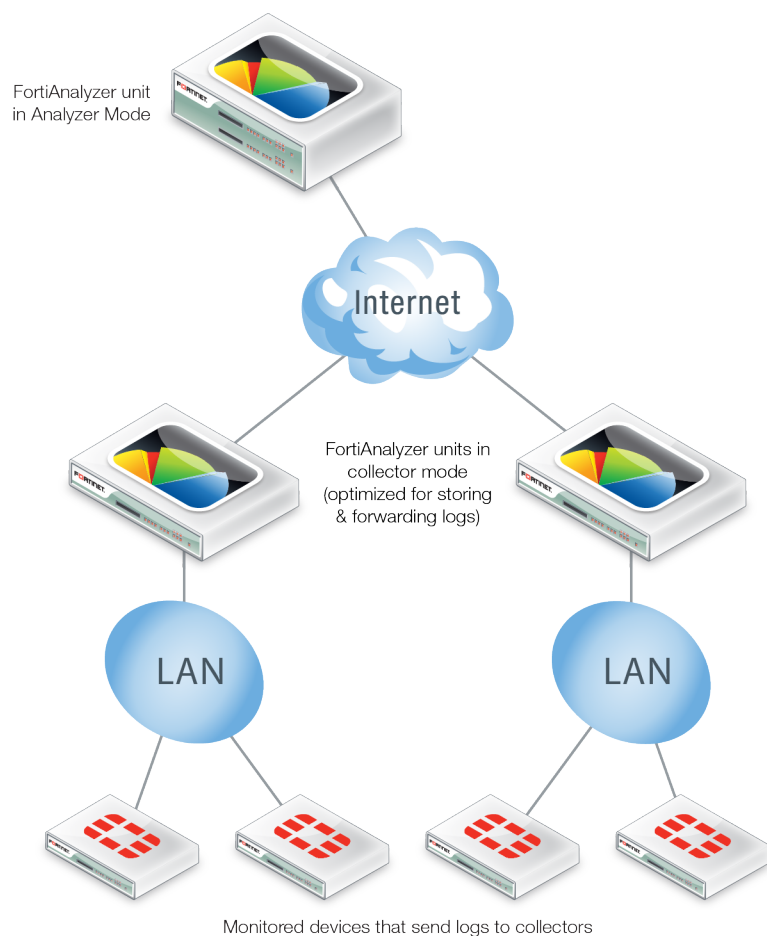


## Analyzer and collector mode

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 below, 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.



### Feature comparison between analyzer and collector mode

Feature	Analyzer Mode	Collector Mode
Event Management	Yes	No
Monitoring devices	Yes	No
Reporting	Yes	No
FortiView/Log View	Yes	No
Device Manager	Yes	Yes
System Settings	Yes	Yes
Log Forwarding	Yes	Yes

## Administrative domains

Administrative domains (ADOMs) enable the `admin` administrator to constrain the access privileges of other FortiAnalyzer unit administrators 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 VDOM for a device.

Enabling ADOMs alters the available functions in the GUI and CLI. Access to the functions depends on whether you are logged in as the `admin` administrator. If you are logged in as the `admin` administrator, you can access all ADOMs. If you are not logged in as the `admin` administrator, access to ADOMs is determined by the settings in your administrator account.

For information on enabling and disabling ADOMs, see [Enabling ADOMs on page 44](#). For information on working with ADOMs, see [Administrative Domains on page 42](#). For information on configuring administrator accounts, see [Administrator Accounts on page 50](#).



ADOMs must be enabled to support FortiCarrier, FortiClient EMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox logging and reporting. See [Administrative Domains on page 42](#).

---

## Log storage

FortiAnalyzer stores logs from managed devices on the FortiAnalyzer disks and in an SQL database. You can control how much storage space to use for logs and how long to store logs.

### SQL database

The FortiAnalyzer unit supports Structured Query Language (SQL) for logging and reporting. The log data is inserted into the SQL database to support data analysis on the *FortiView* pane, *Log View* pane, and *Reports* pane. Remote SQL databases are not supported.

For more information, see [FortiView on page 131](#), [Log View on page 141](#), and [Reports on page 91](#).

The log storage settings define how much FortiAnalyzer disk space to use for the SQL database. See [Log storage on page 20](#).



The SQL database is disabled by default when the FortiAnalyzer unit is operating in collector mode. See [Operation modes on page 17](#).

---

## Compressed logs and indexed logs

While logs are on the FortiAnalyzer unit, they are in one of the following phases, and you can specify how long logs remain in each phase:

- Compressed on hard disks and offline
- Indexed in the SQL database and online

During the compressed phase, logs are compressed and stored on the FortiAnalyzer disks for a specified amount of time for the purpose of retention. While logs are compressed, they are considered offline, and you cannot view

details about the logs on the *FortiView* pane or the *Log View* pane. You also cannot generate reports about the logs on the *Reports* pane.

During the indexed phase, logs are indexed in the SQL database for a specified amount of time for the purpose of analysis. While logs are indexed in the SQL database, they are considered online, and you can view details about the logs on the *FortiView* pane and the *Log View* pane. You can also generate reports about the logs on the *Reports* pane.

You can control how long to retain compressed logs and how long to keep logs indexed in the database by using a data policy.

## Data policy and automatic deletion

A data policy is used to control how long logs remain in the indexed and compressed phases. When ADOMs are enabled, you can specify a unique data policy for each ADOM, which applies to all devices in the ADOM. When ADOMs are disabled, one data policy is applied to all managed devices.

A data policy specifies:

- How long to keep the logs indexed in the database  
When the specified amount of time in the data policy expires, logs are automatically purged from the database, but remain compressed in a log file on the FortiAnalyzer disks.
- How long to keep compressed logs on the FortiAnalyzer disks  
When the specified amount of time in the data policy expires, compressed logs are deleted from the FortiAnalyzer disks.

See also [Configuring log storage on page 80](#).

## Disk utilization for compressed and indexed logs

You can specify how much of the total available FortiAnalyzer disk space to use for log storage. You can specify what ratio of the allotted storage space to use for logs that are indexed in the SQL database and for logs that are stored in a compressed format on the FortiAnalyzer disks. Then you can monitor how quickly device logs are filling up the allotted disk space.



Logs that are indexed in the SQL database require more disk space than logs that are purged from the SQL database, but remain compressed on the FortiAnalyzer disks. The size of an average indexed log is 400 bytes, and the average size of a compressed log is 50 bytes. Keep this difference in mind when specifying the storage ratio for indexed and compressed logs.

When ADOMs are enabled, you can specify disk utilization for each ADOM, and the settings apply to all devices in the ADOM. When ADOMs are disabled, disk utilization settings apply to all managed devices. See also [Configuring log storage on page 80](#).

# Overview

This section provides an overview of configuring and using a FortiAnalyzer unit.



After you configure IP addresses and administrator accounts for the FortiAnalyzer unit, you should log in again by using the new IP address and your new administrator account.

## Configuring FortiAnalyzer

Following is an overview of how to configure a FortiAnalyzer unit to operate in analyzer mode. Analyzer mode is the default mode. For a description of the operating modes, see [Operation modes on page 17](#).

### To configure analyzer mode:

1. Connect to the GUI. See [Connecting to the GUI on page 25](#).
2. Configure IP addresses. See [Configuring ports and administrator access on page 30](#).
3. Configure the RAID level, if the FortiAnalyzer unit supports RAID. See [Configuring RAID on page 38](#).
4. (Optional) Configure administrative domains. See [Configuring ADOMs on page 44](#).
5. Configure administrator accounts. See [Configuring administrator accounts on page 52](#).
6. Add devices to the FortiAnalyzer unit. The devices send logs to the FortiAnalyzer unit. See [Adding devices on page 67](#).
7. Configure log storage. See [Configuring log storage on page 80](#).
8. Configure reports. See [Creating reports on page 94](#).
9. Configure event handlers and alerts. See [Event handlers on page 120](#).
10. Create a system configuration backup. See [Backing up the system configuration on page 188](#).

FortiAnalyzer is configured to collect and analyze the logs it receives from registered FortiGate devices. You are ready to monitor reports, logs, and alerts.

## Configuring FortiAnalyzer units in collector and analyzer modes

You can configure two or more FortiAnalyzer units to work together in collector and analyzer modes. For a description of the operating modes, see [Operation modes on page 17](#). Following is an overview of how to configure two FortiAnalyzer units.

### FortiAnalyzer one - configuring collector mode

Following is an overview of how to configure a FortiAnalyzer unit to operate in collector mode.

**To configure collector mode:**

1. Connect to the GUI. See [Connecting to the GUI on page 25](#).
  2. Configure the operation mode as collector. See [Configuring operation modes on page 155](#).
  3. Configure IP addresses. See [Configuring ports and administrator access on page 30](#).
  4. Configure the RAID level, if the FortiAnalyzer unit supports RAID. See [Configuring RAID on page 38](#).
  5. (Optional) Configure administrative domains (ADOMs). See [Configuring ADOMs on page 44](#).
  6. Configure administrator accounts. See [Configuring administrator accounts on page 52](#).
  7. Add devices to FortiAnalyzer. The devices send logs to the FortiAnalyzer unit. See [Adding devices on page 67](#).
  8. Configure the FortiAnalyzer unit to forward logs to the FortiAnalyzer operating in analyzer mode. See [Overview of configuring aggregation mode on page 164](#).
  9. Back up the system configuration. See [Backing up the system configuration on page 188](#).
- FortiAnalyzer is configured to collect logs from the devices.

## FortiAnalyzer two - configuring analyzer mode

Following is an overview of how to configure a FortiAnalyzer unit to operate in analyzer mode and aggregate logs from FortiAnalyzer units that are operating in collector mode.



Ensure that you allot enough space on the FortiAnalyzer unit in analyzer mode to store the compressed logs and support indexed logs that are forwarded by the FortiAnalyzer unit in collector mode. The FortiAnalyzer unit in analyzer mode requires more disk space for logs because it supports log analysis. For more information, see [Disk utilization for compressed and indexed logs on page 21](#).

**To configure analyzer mode:**

1. Connect to the GUI. See [Connecting to the GUI on page 25](#).
  2. Configure IP addresses. See [Configuring ports and administrator access on page 30](#).
  3. Configure the RAID level, if the FortiAnalyzer unit supports RAID. See [Configuring RAID on page 38](#).
  4. (Optional) Configure administrative domains (ADOMs). See [Configuring ADOMs on page 44](#).
  5. Configure administrator accounts. See [Configuring administrator accounts on page 52](#).
  6. Manually add the FortiAnalyzer unit operating in collector mode to the FortiAnalyzer in analyzer mode. The FortiAnalyzer units operating in collector mode send logs to the FortiAnalyzer unit operating in analyzer mode. See [Adding devices manually on page 69](#).
  7. Configure log storage. See [Configuring log storage on page 80](#).
  8. Configure reports. See [Creating reports on page 94](#).
  9. Configure event handlers. See [Event handlers on page 120](#).
  10. Back up the system configuration. See [Backing up the system configuration on page 188](#).
- FortiAnalyzer is configured to analyze the logs its receives from the registered FortiAnalyzer unit.

## Viewing analyzed log data

After the FortiAnalyzer unit is configured and receiving logs, you can start monitoring data. You can:

- Generate and view reports on the *Reports* pane. See [Reports on page 91](#).
- Generate and view events on the *Event Monitor* pane. See [Event Monitor on page 120](#).
- View summaries of threats, traffic, and more on the *FortiView* pane. See [FortiView on page 131](#).
- View log messages collected by the FortiAnalyzer unit on the *Log View* pane. See [Log View on page 141](#).

## Cannot view the Settings pane

This guide is written for administrators with full privileges, who can access all panes in the FortiAnalyzer GUI, including the *System Settings* pane.

In FortiAnalyzer, administrator privileges are controlled by administrator profiles. Administrators who are assigned profiles with limited privileges might be unable to view some panes in the GUI and might be unable to perform all procedures described in this guide. For more information about administrator profiles, see [Administrator profiles on page 51](#).



If you logged in by using the `admin` administrator account, the *Super\_User* administrator profile is assigned to the `admin` account by default, which gives the `admin` administrator full privileges.

---



# FortiAnalyzer GUI

You can use the GUI to configure most FortiAnalyzer settings, such as the date, time, and the host name. You can also use the GUI to reboot and shut down the FortiAnalyzer unit.

## Connecting to the GUI

For more information on connecting to your specific FortiAnalyzer unit, read that device's [QuickStart Guide](#).

### To connect to the GUI:

1. Connect the FortiAnalyzer unit to a management computer by 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.X
  - 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 click *Login*.
5. If ADOMs are enabled, the *Select an ADOM* pane is displayed. Click an ADOM to select it.  
The home page of tiles is displayed.
6. Click a tile to go to that pane.



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 ports and administrator access on page 30](#).

---



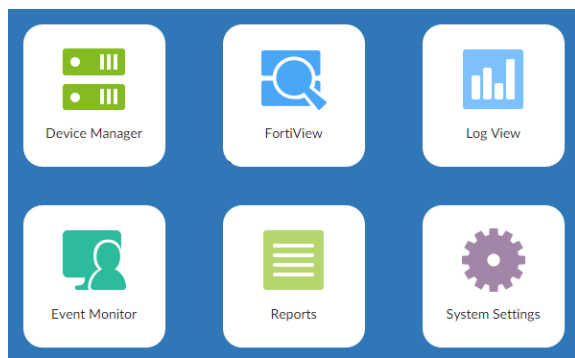
If the URL is correct and you still cannot access the GUI, you may also need to configure static routes. For details, see [Adding a static route on page 31](#).

---

After logging in for the first time, you should create an administrator account for yourself and assign the *Super\_User* profile to it. Then you should log into the FortiAnalyzer unit by using the new administrator account. See [Configuring administrator accounts on page 52](#).

## GUI overview

When you log into the FortiAnalyzer GUI, the following home page of tiles is displayed:



Select one of the following tiles to display the respective pane. The available tiles will vary depending on the privileges of the current user.

<b>Device Manager</b>	Add and manage devices and VDOMs. See <a href="#">Devices on page 67</a> .
<b>FortiView</b>	View summaries of log data in graphical formats. For example, you can view top threats to your network, top sources of network traffic, top destinations of network traffic and so on. For each summary view, you can drill down into details for the event. See <a href="#">FortiView on page 131</a> . This pane is not available when the unit is in Collector mode. See <a href="#">Operation modes on page 17</a> .
<b>Log View</b>	View logs for managed devices. You can display, download, import, and delete logs on this page. You can also define Custom Views and create Log Arrays. See <a href="#">Log View on page 141</a> . This pane is not available when the unit is in Collector mode. See <a href="#">Operation modes on page 17</a> .
<b>Event Monitor</b>	Configure and view events for managed log devices. See <a href="#">Event Monitor on page 120</a> . This pane is not available when the unit is in Collector mode. See <a href="#">Operation modes on page 17</a> .
<b>Reports</b>	Generate reports. You can also configure report templates, schedules, and output profiles, and manage charts and datasets. See <a href="#">Reports on page 91</a> . This pane is not available when the unit is in Collector mode. See <a href="#">Operation modes on page 17</a> .
<b>System Settings</b>	Configure system settings, such as network interfaces, administrators, system time, server settings, and others. You can also perform maintenance and firmware operations. See <a href="#">System Settings on page 151</a> .

The top-right corner of the home page includes an *admin* menu, as well as a *Notification* button, and a *Help* button.

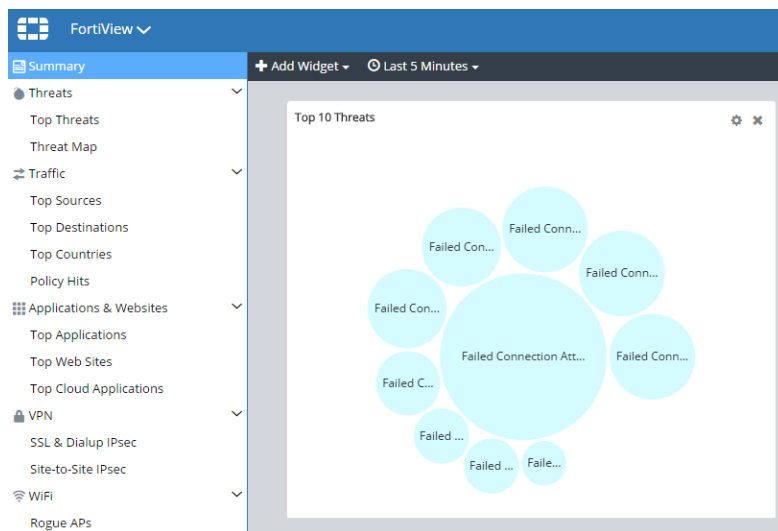


<b>Admin</b>	Click to change the password or log out of the GUI.
<b>Notification</b>	Click to display a list of notifications. Select a notification from the list to take action on the issue.
<b>Help</b>	Click to open the FortiAnalyzer online help or view the <i>About</i> information for your device (Product, Version, and Build Number).

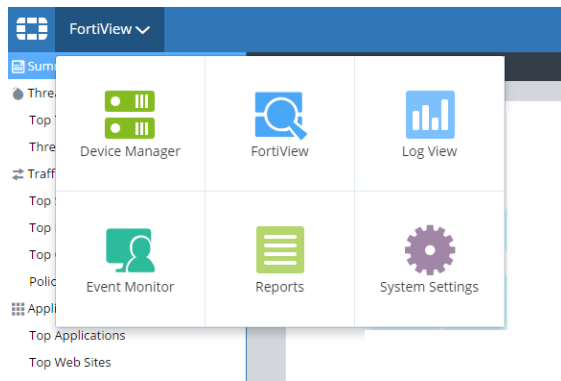
## Panes

In general, panes have four primary parts: the banner, toolbar, tree menu, and content pane.

<b>Banner</b>	Along the top of the page; includes the home button (Fortinet logo), tile menu, ADOM menu (when enabled), admin menu, notifications, and help button.
<b>Tree menu</b>	On the left side of the screen; includes the menus for the selected pane. Not available in <i>Device Manager</i> .
<b>Content pane</b>	Contains widgets, lists, configuration options, or other information, depending on the pane, menu, or options that are selected. Most management tasks are handled in the content pane.
<b>Toolbar</b>	Directly above the content pane; includes options for managing content in the content pane, such as <i>Create New</i> and <i>Delete</i> .

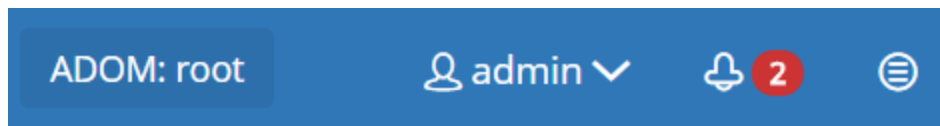


To switch between panes, either select the home button to return to the home page, or select the tile menu then select a new tile.



## Switching between ADOMs

When ADOMs are enabled, you can move between ADOMs by selecting an ADOM from the *ADOM* menu in the banner.

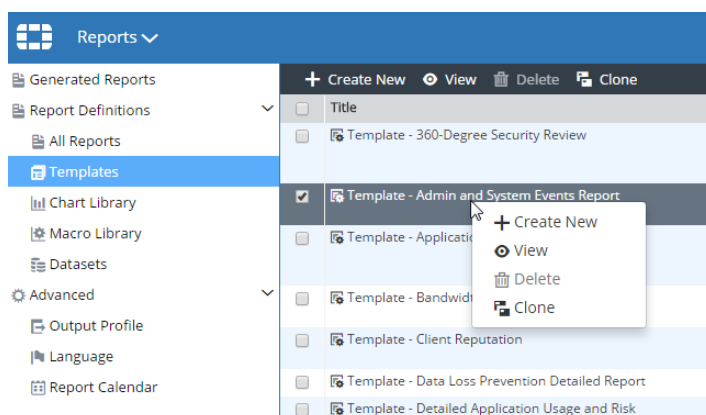


ADOM access is controlled by administrator accounts and the profile assigned to the administrator account. Depending on your account privileges, you might not have access to all ADOMs. See also [Administrator Accounts](#) on page 50.

## Using the right-click menu

Options are sometimes also available by using a right-click menu. You can right-click items in the content pane to display a menu and access the options.

In the following example on the *Reports* pane, you can right-click a template, and select *Create New*, *View*, or *Clone*.



## Restarting and shutting down

Always use the operation options in the GUI or the CLI commands to restart and shut down the FortiAnalyzer system to avoid potential configuration problems.

### To restart the FortiAnalyzer unit from the GUI:

1. Go to *System Settings > Dashboard*.
2. In the *Unit Operation* widget, click the *Restart* button.
3. Enter a message for the event log, then click *OK* to restart the system.

### To restart the FortiAnalyzer unit from the CLI:

1. From the CLI, or in the *CLI Console* widget, enter the following command:  

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

### To shutdown the FortiAnalyzer unit from the GUI:

1. Go to *System Settings > Dashboard*.
2. In the *Unit Operation* widget, click the *Shutdown* button.
3. Enter a message for the event log, then click *OK* to shutdown the system.

### To shutdown the FortiAnalyzer unit from the CLI:

1. From the CLI, or in the *CLI Console* widget, enter the following command:  

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

### To reset the FortiAnalyzer unit:

1. From the CLI, or in the *CLI Console* widget, enter the following command:  

```
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. From the CLI, or in the *CLI Console* widget, enter the following command:  

```
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. All logs will be re-transferred into the database.

# Network

## About the network

The network settings are used to configure one or more ports for the FortiAnalyzer unit. You should also specify what port and methods that administrators can use to access the FortiAnalyzer unit. You can also configure static routes if required.

## Ports

The default port for FortiAnalyzer units is port1. You can use port1 to configure one IP address for the FortiAnalyzer unit, or you can use multiple ports to configure multiple IP addresses for better security.

## Administrative access

The default configuration allows administrative access to one or more of the ports for the FortiAnalyzer unit as described in the QuickStart and installation guides for your device.

You can configure administrative access in IPv4 or IPv6 and include settings for HTTPS, HTTP, PING, SSH (Secure Shell), TELNET, SNMP, Web Service, Aggregator, and FortiManager.

## Restrict administrator access with trusted hosts

You can prevent unauthorized access to the GUI by creating administrator accounts with trusted hosts. With trusted hosts configured, the administrator can only log in to the GUI when working on a computer with the trusted host as defined in the administrator account. For more information, see [Trusted hosts on page 50](#) and [Configuring administrator accounts on page 52](#).

## Configuring the network

### Configuring ports and administrator access

The following port configuration is recommended:

- Use port1 for device log traffic, and disable unneeded services for port1, such as SSH, TELNET, Web Service, and so on.
- Use a second port for administrator access, and enable HTTPs, Web Service, and SSH for this port. Leave other services disabled.

The DNS servers must be on the networks to which the FortiAnalyzer unit connects and should have two different IP addresses.

### To configure IP addresses and administrator access:

1. Go to *System Settings > Network*.

The *System Network Management Interface* pane is displayed. For a description of the fields, see [Network pane on page 32](#).

The screenshot shows the 'System Network Management Interface' configuration pane for 'port1'. The fields and their values are: Name: port1, IP Address/Netmask: 1.1.11.11/255.255.0.0, IPv6 Address: ::0. Under 'Administrative Access', the following services are checked: HTTPS, HTTP, PING, SSH, TELNET, SNMP, Web Service, Aggregator, and FortiManager. Under 'IPv6 Administrative Access', only PING is checked. The Default Gateway is empty, Primary DNS Server is 1.1.1.1, and Secondary DNS Server is 1.1.1.1. An 'Apply' button is at the bottom right. Below the form are three tabs: 'All Interfaces', 'Routing Table', and 'IPv6 Routing Table'.

2. Configure the settings for port1, and click *Apply*.
3. Configure additional ports as needed:
  - a. Select *All Interfaces*.
  - b. Select a port then click *Edit*. The *Edit System Interface* pane is displayed.
  - c. Complete the settings then click *OK*.
  - d. Repeat for each port that you want to configure.

## Adding a static route

### To add a static route:

1. Go to *System Settings > Network*.
2. Click the *Routing Table* button to add an IPv4 static route or the *IPv6 Routing Table* button to add an IPv6 static route.
3. Click the *Create New* button. The *Create New Network Route* pane is displayed. For a description of the fields, see [Create New Network Route pane on page 33](#).
4. Configure the settings, then click *OK* to create the new static route.

## Managing the network

You can view and edit network interfaces and static routes. You can also change administrative access. Some diagnostic tools are also available.

### Viewing network settings

You can view all of the network settings for the FortiAnalyzer unit. The names of the physical interfaces on your FortiAnalyzer unit depend on the model.

If HA operation is enabled, the HA interface has */HA* appended to its name.

To view the Network settings, go to *System Settings > Network*, and click *All Interfaces*, *Routing Table*, or *IPv6 Routing Table*.

## Editing network settings

### To edit a network setting:

1. Go to *System Settings > Network*, and click *All Interfaces*, *Routing Table*, or *IPv6 Routing Table*.
2. Select an entry, and click *Edit*. For a description of the fields, see [Edit System Interface pane on page 33](#).
3. Configure the settings as required, then click *OK*.

## Changing administrative access

### To change administrative access:

1. Go to *System Settings > Network*.  
By default, port1 settings are displayed. You can configure administrative access for a different interface. Click *All Interfaces*, and then select the interface from the list.
2. Set the IPv4 *IP Address/Netmask* or the *IPv6 Address*.
3. Select one or more *Administrative Access* types for the interface, and set the default gateway and Domain Name System (DNS) servers.
4. Click *Apply*.

## Disabling ports

You can enable and disable ports. When a port is enabled, it accepts network traffic. When a port is disabled, no network traffic is accepted.

### To disable ports:

1. Go to *System Settings > Network*.
2. Click *All Interfaces*.
3. Select a port, then click *Edit*.
4. Beside *Status*, click the *Disable* button, then click *OK*.

## Network references

### Network pane

Following is a description of the fields on the *System Settings > Network* pane when creating an interface.



Field	Description
IP Address/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: <i>HTTPS</i> , <i>HTTP</i> , <i>PING</i> , <i>SSH</i> , <i>TELNET</i> , <i>SNMP</i> , <i>Web Service</i> , <i>Aggregator</i> , and <i>FortiManager</i> .
IPv6 Administrative Access	Select the allowed IPv6 administrative service protocols from: <i>HTTPS</i> , <i>HTTP</i> , <i>PING</i> , <i>SSH</i> , <i>TELNET</i> , <i>SNMP</i> , <i>Web Service</i> , <i>Aggregator</i> , and <i>FortiManager</i> .
Default Gateway	Type the default gateway associated with this interface
Primary DNS Server	Type the primary DNS server IP address.
Secondary DNS Server	Type the secondary DNS server IP address.
All Interfaces	Opens the network interface list.
Routing Table	Opens the routing table.
IPv6 Routing Table	Opens the IPv6 routing table.

## Create New Network Route pane

Following is a description of the fields on the *System Settings > Network* pane when creating a static route.

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

## Edit System Interface pane

Following is a description of the fields on the *System Settings > Network* page when editing a network interface.

Field	Description
Name	Displays the name of the interface.

Field	Description
Alias	Type an alias for the port to make it easily recognizable.
IP Address/Netmask	Type the IP address and netmask for the interface.
IPv6 Address	Type the IPv6 address for the interface.
Administrative Access	Select the services to allow on this interface. Any interface that is used to provide administration access to the FortiAnalyzer unit will require at least HTTPS or HTTP for GUI 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 GUI access, or SSH for CLI access.
Service Access	Select if FortiGate Updates services are allowed access on this interface. By default, service access is disabled on all ports.
Status	Enable or disable the interface. Click <i>Enable</i> to enable the interface and allow the interface to accept network traffic. Click <i>Disable</i> to disable the interface.

# RAID

## About RAID

RAID helps to divide data storage over multiple disks, providing increased data reliability. For FortiAnalyzer units that contain multiple hard disks, you can configure the RAID array for capacity, performance, and availability.

If the FortiAnalyzer device supports RAID, you can choose the RAID level for the device on the *System Settings > RAID Management* pane.



The *RAID Management* tree menu is only available on FortiAnalyzer devices that support RAID.

---

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

## RAID 60

A RAID 60 (6+ 0) array combines the straight, block-level striping of RAID 0 with the distributed double parity of RAID 6.

- 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

Model	RAID Type	RAID Level	Hot Swappable
FAZ-100C	-	-	-
FAZ-200D	-	-	-

Model	RAID Type	RAID Level	Hot Swappable
FAZ-300D	Software RAID	Linear, 0, 1	No
FAZ-400C	-	-	-
FAZ-1000C	Software RAID	Linear, 0, 1, 10	No
FAZ-1000D	Software RAID	Linear, 0, 1, 5, 10	No
FAZ-3000D	Hardware RAID	0, 1, 1 +Spare, 5, 5 +Spare, 6, 6 +Spare, 10, 50, 60	Yes
FAZ-3000E	Hardware RAID	0, 1, 1 +Spare, 5, 5 +Spare, 6, 6 +Spare, 10, 50, 60	Yes
FAZ-3500E	Hardware RAID	0, 1, 1 +Spare, 5, 5 +Spare, 6, 6 +Spare, 10, 50, 60	Yes
FAZ-3900E	Hardware RAID	0, 1, 1 +Spare, 5, 5 +Spare, 6, 6 +Spare, 10, 50, 60	Yes
FAZ-4000B	Hardware RAID	0, 5, 5 +Spare, 6, 6 +Spare, 10, 50, 60	Yes
FAZ-VM	-	-	-
FAZ-VM64, FAZ-VM64-HV	-	-	-

## Configuring RAID

### To configure the RAID level:

1. Go to *System Settings > RAID Management*.
2. Beside *RAID Level*, click *Change*. The *RAID Settings* dialog box is displayed.
3. From the *RAID Level* list, select a new RAID level, and click *OK*.

The FortiAnalyzer unit reboots. Depending on the selected RAID level, it may take a significant amount of time to generate the RAID array.



If you change the RAID settings, all data will be deleted.

## Managing RAID

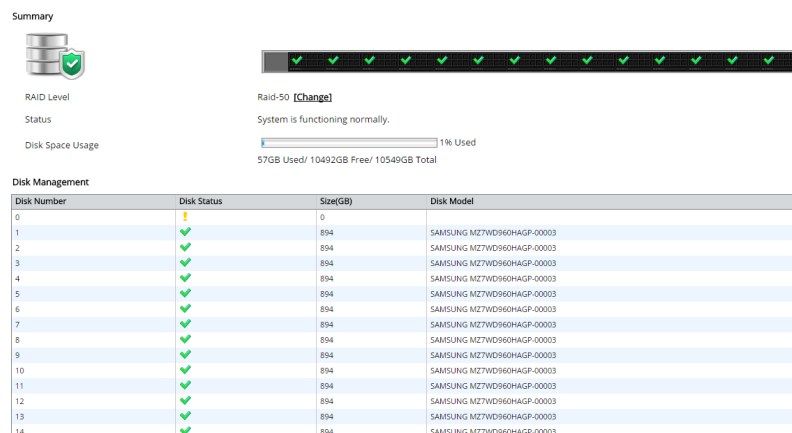
You can monitor RAID status, swap hard disks, and in some cases, add new disks to the FortiAnalyzer unit.

## Monitoring RAID status

The *Alert Message Console* widget, which is located in *System Settings > Dashboard*, provides detailed information about any RAID array failures. For more information, see [Viewing alert messages on page 155](#).

### To view RAID status:

Go to *System Settings > RAID Management*. The *RAID Management* pane displays the status of each disk in the RAID array, including the disk's RAID level. You can also see how much disk space is being used. For a description of the fields, see [RAID references on page 40](#).



## 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, which is 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 [Viewing alert messages on page 155](#).



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.

**To hot-swap a hard disk on a device that supports hardware RAID:**

Remove the faulty hard disk, and replace it with a new one.

The FortiAnalyzer unit automatically adds the new disk to the current RAID array. The status appears on the console. The *RAID Management* pane displays a green check mark icon for all disks, and the *Status* area displays 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.
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, shut down the device (see [Restarting and shutting down on page 29](#)), install the disk or disks, and then restart the device.
4. Configure the RAID level. See [Configuring RAID on page 38](#).
5. If you have backed up the log data, restore the data.

**RAID references****RAID Management pane**

Following is a description of the fields on the *System Settings > RAID Management* pane.

Field	Description
<b>Summary</b>	Displays summary information about the RAID array.
<b>Graphic</b>	Displays the position and status of each disk in the RAID array. Hover over each disk to view status details.
<b>RAID Level</b>	Displays the selected RAID level. Click <i>Change</i> to change the selected RAID level. When you change the RAID settings, all data is deleted.



Field	Description
<b>Status</b>	Displays the overall status of the RAID array
<b>Disk Space Usage</b>	Displays the total size of the disk space, how much disk space is used, and how much disk space is free.
<b>Disk Management</b>	Displays information about each disk in the RAID array.
<b>Disk Number</b>	Identifies the disk number for each disk in the RAID array
<b>Disk Status</b>	<p>Displays the status of each disk in the RAID array</p> <ul style="list-style-type: none"> <li>• <i>Ready</i>: The hard drive is functioning normally.</li> <li>• <i>Rebuilding</i>: 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.</li> <li>• <i>Initializing</i>: The FortiAnalyzer unit is writing to all the hard drives in the device in order to make the array fault tolerant.</li> <li>• <i>Verifying</i>: The FortiAnalyzer unit is ensuring that the parity data of a redundant drive is valid.</li> <li>• <i>Degraded</i>: The hard drive is no longer being used by the RAID controller.</li> <li>• <i>Inoperable</i>: 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.</li> </ul>
<b>Size (GB)</b>	Displays the size in GB of each disk in the RAID array
<b>Disk Model</b>	Displays the model number of each disk in the RAID array

# Administrative Domains

## About ADOMs

FortiAnalyzer administrative domains (ADOMs) are used to create groupings of devices and VDOMs for configured administrators to monitor and manage. FortiAnalyzer can manage a large number of devices and VDOMs. This enables administrators to maintain managed devices and VDOMs specific to their geographic location or business division.

Each FortiAnalyzer ADOM also specifies how much FortiAnalyzer disk space to use for its logs and how long to store its logs. You can monitor disk utilization for each ADOM and adjust storage settings for logs as needed.

Each administrator is tied to an administrative domain (ADOM). When an administrator logs in, the administrator sees only those devices or VDOMs configured for that administrator and ADOM. The one exception is administrative accounts assigned the *Super\_User* profile. These administrators can see and maintain all administrative domains and the devices within those domains.

Administrative domains are disabled by default, and enabling and configuring the domains can only be performed by administrators with accounts that are assigned the *Super\_User* profile.



ADOMs must be enabled to support FortiCarrier, FortiClient EMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox logging and reporting.

---



ADOMs must be enabled to support non-FortiGate logging and reporting. When a non-FortiGate device is registered with the FortiAnalyzer unit, the device is added to its respective default ADOM and is visible in the left tree menu.

---

## How ADOMs affect the GUI

When ADOMs are enabled, the *Device Manager*, *FortiView*, *Log View*, *Event Monitor*, and *Reports* tabs are displayed per ADOM. You select the ADOM for which you want to view information when you log into the FortiAnalyzer unit. See also [Switching between ADOMs on page 28](#).

## Default ADOMs

FortiAnalyzer includes default ADOMs. The default ADOMs are for specific types of devices. When you add one or more of these devices to FortiAnalyzer, the devices are automatically added to the appropriate ADOM, and then the ADOM is visible for selection. When a default ADOM contains no devices, the ADOM is not visible for selection.

For example, when you add a FortiClient EMS device to FortiAnalyzer, the FortiClient EMS device is automatically added to the default FortiClient ADOM. After the FortiClient ADOM contains a FortiClient EMS device, the FortiClient ADOM is visible for selection when you log into FortiAnalyzer or when you switch between ADOMs.

You can view all of the ADOMs, including default ADOMs without devices, on the *System Settings > All ADOMs* page.

## FortiClient support and ADOMs

FortiClient logs are stored with the device to which the FortiClient endpoint is registered.

For example, when endpoints are registered to a FortiGate device, you view FortiClient logs by viewing the FortiGate device. If ADOMs are enabled, you view FortiClient logs by viewing the ADOM for the FortiGate device.

When endpoints are registered to a FortiClient EMS server, you view FortiClient logs by viewing the FortiClient ADOM. ADOMs must be enabled to support FortiClient EMS devices.

## Considerations for creating ADOMs

Keep the following considerations in mind when creating ADOMs:

- You can only create ADOMs when you are using an administrator account that is assigned the *Super\_User* administrative profile.
- The maximum number of ADOMs you can create depends on the specific FortiAnalyzer system model. Please refer to the FortiAnalyzer data sheet for information on the maximum number of devices and ADOMs that your model supports.
- You must add a device to only one ADOM. You cannot add a device to multiple ADOMs.
- You cannot add FortiGate and FortiCarrier devices to the same ADOM. FortiCarrier devices are added to a specific, default FortiCarrier ADOM.
- You can add one or more VDOMs from a FortiGate device to one ADOM. If you want to add individual VDOMs from a FortiGate device to different ADOMs, you must first enable ADOMs in advanced device mode.
- You can configure how an ADOM handles log files from its devices. For example, you can configure how much FortiAnalyzer disk space that an ADOM can use for logs, and then monitor the fullness of the allotted disk space. You can also specify how long to keep logs indexed in the SQL database for analysis and how long to keep logs stored in a compressed format.

## ADOM device modes and VDOM support

An ADOM has two device modes to support VDOMs: normal and advanced.

In normal device mode, you must assign the FortiGate unit and all of its VDOMs to a single ADOM. You cannot assign different FortiGate VDOMs to multiple FortiAnalyzer ADOMs.

In advanced device mode, you can assign different VDOMs from the same FortiGate unit to multiple ADOMs. This allows you to use the *FortiView*, *Event Management*, and *Reports* tabs to analyze data for individual VDOMs. See [Enabling advanced ADOM device mode on page 44](#).



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.

## Configuring ADOMs

### Enabling ADOMs

You must enable the ADOM feature before you can create ADOMs.

**To enable the ADOM feature:**

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, toggle the *Administrative Domain* switch to *On*.
3. Type your username and password when prompted.

### Enabling advanced ADOM device mode

You must enable ADOMs before you can enable advanced ADOM device mode.

Normal ADOM device mode is the default setting. Advanced ADOM device mode is only required in certain situations, see [ADOM device modes and VDOM support](#).

**To enable advanced ADOM device mode:**

Go to *System Settings > Advanced > Advanced Settings*, select *Advanced* in the *ADOM Mode* field, then click *Apply*.

Alternatively, use the following command in the CLI:

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

### Creating ADOMs

When you create ADOMs, you can specify what devices to include in the ADOM. You can also specify how much FortiAnalyzer disk space that the ADOM can use for its logs. You can also specify how long to index logs in the SQL database to support analysis and how long to store compressed logs for retention.

**To create an ADOM:**

1. Go to *System Settings > All ADOMs*.
2. Select *Create New* from the toolbar. For a description of the fields, see [Create or Edit ADOM pane on page 47](#).

3. Set the options then select **OK** to create the ADOM.
4. Configure the data policy and disk utilization for the ADOM see .

## Assigning devices to ADOMs

The *Super\_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 ADOMs:

1. Go to *System Settings > All ADOMs*.
2. Select an ADOM then click *Edit* in the toolbar.
3. Click *Select Device*. The *Device Selection* dialog box will open on the right side of the screen.
4. Select the devices that you want to associate with the ADOM, then click *Close* to close the box.  
If the ADOM mode is *Advanced* you can add separate VDOMs to the ADOM as well as units.
5. When you are done, click *OK*. The selected devices are moved to the ADOM.

## Assigning administrators to ADOMs

Administrators that are assigned the *Super\_Admin* administrator profile 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 [Creating ADOMs on page 44](#).

### To assign administrator to ADOMs:

1. Log in to the device as *admin*. Other administrators cannot configure administrator accounts when ADOMs are enabled.
2. Go to *System Settings > Admin > Administrator*.
3. Select an administrator account, and select *Edit*.



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

4. Edit the *Administrative Domain* field as required, either assigning or excluding specific ADOMs.
5. Select *OK* to apply your changes.

## Managing ADOMs

You can manage ADOMs by navigating to *System Settings > All ADOMs*. Options are available in the toolbar. Some options are available in the right-click menu. Right-click an ADOM to display the menu.

Option	Description
<b>Create New</b>	Create a new ADOM
<b>Edit</b>	Edit the selected ADOM.
<b>Delete</b>	Deletes the selected ADOM. You cannot delete default ADOMs, such as the root.
<b>Switch to ADOM</b>	Switches to ADOM.
<b>Expand Devices</b>	Expands the ADOM to show the device list within the ADOM.
<b>Collapse Devices</b>	Collapses the device list within the ADOM

## Viewing all ADOMs

The *All ADOMs* menu item displays all the ADOMs configured on the device, and provides the option to create new ADOMs. Clicking a column heading will sort the list based on that heading. It is only visible if ADOMs are enabled, see [Enabling ADOMs on page 44](#). For a description of the fields, see [All ADOMs pane on page 47](#).



FortiAnalyzer 5.2.0 and later supports FortiGate, FortiCache, FortiCarrier, FortiClient, FortiDDoS, FortiMail, FortiSandbox, FortiWeb, Syslog, and others ADOM types.

## Disabling advanced ADOM mode

**To disable advanced ADOM mode:**

1. Ensure no FortiGate VDOMs are assigned to an ADOM.
2. Go to *System Settings > Advanced > Advanced Settings*.
3. In the *ADOM Mode* field, select *Normal*, then select *Apply*.

## Disabling ADOMs



The default ADOMs cannot be disabled.

### To disable the ADOM feature:

1. Remove all log devices from all non-root ADOMs:
  - a. Ensure you are in the correct *ADOM*.
  - b. Navigate to *Device Manager*.
  - c. Select *Delete*.
2. Delete all non-root ADOMs:
  - a. Go to *System Settings > All ADOMs*.
  - b. Select each non-root ADOM and select *Delete*.
  - c. Select *OK* in the dialog box to delete the ADOM.
3. Disable ADOMs:
  - a. Go to *System Settings > Dashboard*.
  - b. In the System Information widget, select *OFF* next to *Administrative Domain* to disable ADOMs.

## ADOM references

### All ADOMs pane

Following is a description of the options on the *System Settings > All ADOMs* pane.

Field	Description
<b>Name</b>	Displays the name of the ADOM. ADOMs are listed in the following groups: <i>Central Management</i> and <i>Other Device Types</i> . You can expand and hide the groups to view the ADOMs contained in the group.
<b>Firmware Version</b>	Displays the version of devices the ADOM contains.
<b>Allocated Storage</b>	The amount of hard drive storage space allocated to the ADOM.
<b>Device</b>	Displays how many devices that the ADOM contains. You can display and hide the names of the devices in the ADOM by clicking the triangle.

### Create or Edit ADOM pane

Following is a description of the options available on the *Create ADOM* and *Edit ADOM* panes.

Field	Description
<b>Name</b>	Type a unique name for the ADOM. The ADOM name cannot be edited when editing an ADOM.
<b>Type</b>	Select the type of device for which you are creating an ADOM. Although you can create a different ADOM for each type of device, FortiAnalyzer does not enforce this setting . The ADOM type cannot be edited when editing an ADOM.
<b>Version</b>	Select the version of device for which you are creating an ADOM. Although you can create a different ADOM for each version of device, FortiAnalyzer does not enforce this setting. For example, if you have FortiGate version 5.2 devices and FortiGate version 5.4 devices, you can create one ADOM for the version 5.2 devices and one ADOM for the version 5.4 devices. The ADOM version cannot be edited when editing an ADOM.
<b>Devices</b>	Displays all of the devices in the ADOM in a dialog box.
<b>Select Device</b>	Add devices to the ADOM.
<b>Search</b>	Type a device name then press <i>Enter</i> to search for the device in the device list.
<b>Data Policy</b>	Specify how long to keep logs in the indexed and compressed states.
<b>Keep Indexed Logs for Analytics</b>	Specify how long to keep logs in the indexed state. During the indexed state, logs are indexed in the SQL database for the specified amount of time, and you can view information about the logs on the <i>FortiView</i> , <i>Event Monitor</i> , and <i>Reports</i> tabs. After the specified amount of time expires, logs are automatically purged from the SQL database.
<b>Keep Compressed Logs for Retention</b>	Specify how long to keep logs in the compressed state. During the compressed state, logs are stored in a compressed format on the FortiAnalyzer unit. When logs are in the compressed state, you cannot view information about the log messages on the <i>FortiView</i> , <i>Event Monitor</i> , and <i>Reports</i> tabs. After the specified amount of time expires, compressed logs are automatically deleted from the FortiAnalyzer unit.
<b>Disk Utilization</b>	Specify how much FortiAnalyzer disk space to use for logs.
<b>Maximum Allowed</b>	Specify a maximum amount of FortiAnalyzer disk space to use for logs, and select the unit of measure. You can view the total available space for the FortiAnalyzer unit. For more info about the maximum available space for each FortiAnalyzer unit, see <a href="#">FortiAnalyzer disk space allocation on page 76</a> .



Field	Description
<b>Indexed: Compressed</b>	Specify how much of the allotted space to use for indexed and compressed logs. Indexed logs require more space than compressed logs. For example, a setting of 70% and 30% indicates that 70% of the allotted disk space will be used indexed logs, and 30% of the allotted space will be used for compressed logs. Select the <i>Modify</i> check box to change the setting.
<b>Alert and Delete When Usage Reaches</b>	Specify at what fullness you want alert messages to be generated and compressed logs to be automatically deleted. The oldest compressed logs are deleted first.

# Administrator Accounts

## About administrator accounts

Administrator accounts are used to control administrator access to the FortiAnalyzer unit. Local and remote authentication is supported as well as two-factor authentication.

FortiAnalyzer includes administrator profiles that define different types of administrators and what level of access each type of administrator has to devices connected to the FortiAnalyzer unit and to the FortiAnalyzer features. You can assign an administrator profile to each administrator account.

When you create an administrator account in FortiAnalyzer, you can specify the following items for the administrator:

- Authentication method
- Administrator profile
- ADOMs that the administrator can access

You can configure and monitor administrator access to the FortiAnalyzer unit from *System Settings > Admin*.

## Administrator accounts

Administrator accounts control who can access the FortiAnalyzer unit, the method of authentication used for the administrator, the profile associated with the administrator, and the ADOM associated with the administrator.

## How ADOMs affect administrator access

When ADOMs are enabled, administrators can access only the ADOMs listed in the administrator account that is associated with the administrator.

## 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 GUI and to the CLI when accessed through SSH. CLI access through the console connector is not affected.



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

---

## Administrator profiles

Administrator profiles are used to limit administrator access privileges to devices or system features. The administrator profiles restrict access to both the GUI and CLI. You can assign a profile to an administrator when you create the administrator account.

### Predefined profiles

FortiAnalyzer includes the following predefined profiles that you can assign to administrators:

<b>Restricted_User</b>	Restricted user profiles have no System Privileges enabled, and have read-only access for all Device Privileges.
<b>Standard_User</b>	Standard user profiles have no System Privileges enabled, but have read/write access for all Device Privileges.
<b>Super_User</b>	Super user profiles have all system and device privileges enabled. It cannot be edited.



*Restricted\_User* and *Standard\_User* admin profiles do not have access to the *System Settings* tab. An administrator with either of these admin profiles will see a change password icon in the navigation pane.

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.

Feature	Predefined Administrator Profiles		
	Super User	Standard User	Restricted User
System Settings / <code>system-setting</code>	Read-Write	None	None
Administrator Domain / <code>adom-switch</code>	Read-Write	Read-Write	None
Device Manager / <code>device-manager</code>	Read-Write	Read-Write	Read-Only
Add/Delete Devices/Groups / <code>device-op</code>	Read-Write	Read-Write	None
FortiView / <code>realtime-monitor</code>	Read-Write	Read-Write	Read-Only
Event Management / <code>event-management</code>	Read-Write	Read-Write	Read-Only
Reports / <code>report-viewer</code>	Read-Write	Read-Write	Read-Only
CLI Only Settings			

Feature	Predefined Administrator Profiles		
	Super User	Standard User	Restricted User
profileid	Super_User	Standard_User	Restricted_User
device-wan-link-load-balance	Read-Write	Read-Write	Read-Only
device-ap	Read-Write	Read-Write	Read-Only
device-forticlient	Read-Write	Read-Write	Read-Only
log-viewer	Read-Write	Read-Write	Read-Only

You cannot delete these profiles, but standard and restricted user profiles can be edited. You can also create new profiles as required.



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

## Configuring administrator accounts

You need the following information to create an administrator account:

- What authentication method the administrator will use to log into the FortiAnalyzer unit. Local and remote authentication methods are supported.
- What administrator profile you want to assign to the account
- What ADOMs you want the administrator to access, if using ADOMs
- The trusted host address and network mask, if using trusted hosts

### To create a new administrator account:

1. Go to *System Settings > Admin > Administrator* and select *Create New* from the toolbar. For a description of the fields, see [Create Administrator page on page 64](#).

2. Configure the settings, then select **OK** to create the new administrator account.

## Managing administrator accounts

You can manage administrator accounts by navigating to *System Settings > Admin > Administrator*.

Option	Description
<b>Create New</b>	Create a new administrator account.
<b>Edit</b>	Edit the selected administrator account.
<b>Delete</b>	Delete the selected administrator account. You cannot delete the default <i>admin</i> administrator account.

## Viewing administrator accounts

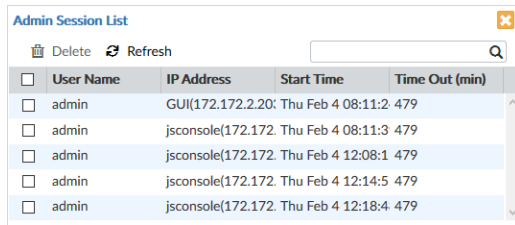
Go to *System Settings > Admin > Administrator* to view the list of administrators. Only the default *admin* administrator account can see the complete administrators list. If you do not have certain viewing privileges, you will not see the administrator list.

## Viewing administrators logged into the FortiAnalyzer unit

You can view the list of administrators logged into the FortiAnalyzer unit and disconnect administrators if necessary.

### To view logged in administrators on the FortiAnalyzer unit:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, in *Current Administrators* field, click the *Current Session List* button. The list of current administrator sessions opens.



The screenshot shows a widget titled "Admin Session List" with a toolbar containing "Delete" and "Refresh" buttons and a search icon. Below the toolbar is a table with the following data:

<input type="checkbox"/>	User Name	IP Address	Start Time	Time Out (min)
<input type="checkbox"/>	admin	GUI(172.172.2.20)	Thu Feb 4 08:11:2	479
<input type="checkbox"/>	admin	jsconsole(172.172.2.20)	Thu Feb 4 08:11:3	479
<input type="checkbox"/>	admin	jsconsole(172.172.2.20)	Thu Feb 4 12:08:1	479
<input type="checkbox"/>	admin	jsconsole(172.172.2.20)	Thu Feb 4 12:14:5	479
<input type="checkbox"/>	admin	jsconsole(172.172.2.20)	Thu Feb 4 12:18:4	479

3. Click the close button to return to the normal widget.

## Disconnecting administrators from the FortiAnalyzer unit

### To disconnect an administrator:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, in the *Current Administrators* field, click the *Current Sessions List* button. The list of current administrator sessions appears.
3. Select the administrator session or sessions that you want to disconnect, then select *Delete* from the toolbar.
4. Click *OK* to confirm deletion of the session or sessions.

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 profiles

### Managing administrator profiles

You can manage administrator profiles from the *System Settings > Admin > Profile* page. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click an administrator profile to display the menu.

Option	Description
<b>Create New</b>	Create a new administrator profile.
<b>Edit</b>	Edit an administrator profile. The <i>Super_User</i> profile cannot be deleted.
<b>Delete</b>	Delete the selected administrator profile. You can only delete custom profiles that are not applied to any administrators. You cannot delete the default administrator profiles: <i>Restricted_User</i> , <i>Standard_User</i> , and <i>Super_User</i> .

### Creating custom administrator profiles

You can create custom profiles, and edit existing profiles, including the predefined profiles, as required. Only administrators with full system privileges can edit the administrator profiles.

**To create a custom profile:**

1. Go to *System Settings > Admin > Profile*.
2. Select *Create New*. For a description of the fields, see [Create Administrator Profile page on page 65](#).
3. Configure the settings, then select *OK* to create the new profile.

## Remote authentication servers

The FortiAnalyzer system supports remote authentication of administrators using Remote Authentication Dial-in User (RADIUS), Lightweight Directory Access Protocol (LDAP), and Terminal Access Controller Access-Control System (TACACS+) servers. To use this feature, you must configure the appropriate server entries in the FortiAnalyzer unit for each authentication server in your network. LDAP servers can be linked to all ADOMs or to specific ADOMs.

### Managing remote authentication servers

You can manage remote authentication servers from the *System Settings > Admin > Remote Auth Server* page. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a remote authentication server to display the menu.

Option	Description
<b>Create New</b>	Create a new remote authentication server.
<b>Edit</b>	Edit a remote authentication server. You cannot change the name field when editing a remote authentication server.
<b>Delete</b>	Delete the selected remote authentication server. You cannot delete a remote authentication server entry if administrators are using it.

### Adding an LDAP server

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 an LDAP server:**

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

**New LDAP Server**

Name

Server Name/IP

Port

Common Name Identifier

Distinguished Name

Bind Type

Secure Connection ☒ Enable

Protocol

Certificate

Administrative Domain

3. Configure the following information:

<b>Name</b>	Enter a name to identify the LDAP server.
<b>Server Name/IP</b>	Enter the IP address or fully qualified domain name of the LDAP server.
<b>Port</b>	Enter the port for LDAP traffic. The default port is 389.
<b>Common Name Identifier</b>	The common name identifier for the LDAP server. Most LDAP servers use <i>cn</i> . However, some servers use other common name identifiers such as <i>uid</i> .
<b>Distinguished Name</b>	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. Select the query icon to query the distinguished name.
<b>Bind Type</b>	Select the type of binding for LDAP authentication from the drop-down list. One of: <i>Simple</i> , <i>Anonymous</i> , or <i>Regular</i> .
<b>User DN</b>	Enter the user distinguished name. This option is available when the <i>Bind Type</i> is set to <i>Regular</i> .
<b>Password</b>	Enter the user password. This option is available when the <i>Bind Type</i> is set to <i>Regular</i> .
<b>Secure Connection</b>	Select to use a secure LDAP server connection for authentication.
<b>Protocol</b>	Select the secure connection protocol, <i>LDAPS</i> or <i>STARTTLS</i> . This option is only available when <i>Secure Connection</i> is selected.
<b>Certificate</b>	Select a CA certificate. This option is only available when <i>Secure Connection</i> is selected.
<b>Administrative Domain</b>	Select either <i>All ADOMs</i> or <i>Specify</i> to select which ADOMs to link to the LDAP server. Select <i>Specify</i> and then select the add icon to add Administrative Domains. Select the remove icon to remove an Administrative Domain.

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



## Adding a RADIUS server

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 *Create New* in the toolbar, and select *RADIUS Server* from the drop-down list.

3. Configure the following settings:

<b>Name</b>	Enter a name to identify the RADIUS server.
<b>Server Name/IP</b>	Enter the IP address or fully qualified domain name of the RADIUS server.
<b>Port</b>	Enter the port for RADIUS traffic. The default port is 1812. Some RADIUS servers use port 1645.
<b>Server Secret</b>	Enter the RADIUS server secret.
<b>Secondary Server Name/IP</b>	Enter the IP address or fully qualified domain name of the secondary RADIUS server.
<b>Secondary Server Secret</b>	Enter the secondary RADIUS server secret.
<b>Authentication Type</b>	Enter the authentication type the RADIUS server requires: <i>ANY</i> , <i>PAP</i> , <i>CHAP</i> , or <i>MSv2</i> . The default setting of <i>ANY</i> has the FortiAnalyzer unit try all the authentication types.

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

## Adding a TACACS+ server

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 *Create New* in the toolbar, and select *TACACS+ Server* from the drop-down list.

The screenshot shows a 'New TACACS+ Server' dialog box. It contains the following fields: 'Name' (text input), 'Server Name/IP' (text input), 'Port' (text input with '49' and a spinner), 'Server Key' (text input), and 'Authentication Type' (dropdown menu). At the bottom, there are 'OK' and 'Cancel' buttons.

3. Configure the following information:

<b>Name</b>	Enter a name to identify the TACACS+ server.
<b>Server Name/IP</b>	Enter the IP address or fully qualified domain name of the TACACS+ server.
<b>Port</b>	Enter the port for TACACS+ traffic. The default port is 49.
<b>Server Key</b>	Enter the key to access the TACACS+ server. The server key can be a maximum of 16 characters in length.
<b>Authentication Type</b>	Enter the authentication type the TACACS+ server requires: <i>AUTO</i> , <i>ASCII</i> , <i>PAP</i> , <i>CHAP</i> , or <i>MSCHAP</i> . The default value is <i>AUTO</i> .

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

## Two-factor authentication

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

- FortiAnalyzer
- FortiAuthenticator
- FortiToken

### Configuring FortiAuthenticator

The following instructions describes the steps required on your FortiAuthenticator device to configure two-factor authentication for administrator logins.



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

**To create a new local user:**

1. Go to *Authentication > User Management > Local Users*.
2. Select *Create New* from the toolbar.
3. Configure the following settings:

<b>Username</b>	Enter a user name for the local user.
<b>Password creation</b>	Select Specify a password from the drop-down list.
<b>Password</b>	Enter a password. The password must be a minimum of 8 characters.
<b>Password confirmation</b>	Re-enter the password. The passwords must match.
<b>Allow RADIUS authentication</b>	Enable to allow RADIUS authentication.
<b>Role</b>	Select the role for the new user.
<b>Enable account expiration</b>	Optionally, select to enable account expiration. For more information see the <i>FortiAuthenticator Administration Guide</i> .

4. Select *OK* to continue.

5. Configure the following settings:

<b>Disabled</b>	Select to disable the local user.
<b>Password-based authentication</b>	Leave this option selected. Select <i>[Change Password]</i> to change the password for this local user.
<b>Token-based authentication</b>	Select to enable token-based authentication.
<b>Deliver token code by</b>	Select to deliver token by FortiToken, Email or SMS. Select <i>Test Token</i> to test the token.
<b>Allow RADIUS authentication</b>	Select to allow RADIUS authentication.

<b>Enable account expiration</b>	Optionally, select to enable account expiration. For more information see the <i>FortiAuthenticator Administration Guide</i> .
<b>User Role</b>	
<b>Role</b>	Select either <i>Administrator</i> or <i>User</i> .
<b>Full Permission</b>	Select to allow Full Permission, otherwise select the admin profiles to apply to the user. This option is only available when <i>Role</i> is <i>Administrator</i> .
<b>Web service</b>	Select to allow Web service, which allows the administrator to access the web service via a REST API or by using a client application. This option is only available when <i>Role</i> is <i>Administrator</i> .
<b>Restrict admin login from trusted management subnets only</b>	Select to restrict admin login from trusted management subnets only, then enter the trusted subnets in the table. This option is only available when <i>Role</i> is <i>Administrator</i> .
<b>Allow LDAP Browsing</b>	Select to allow LDAP browsing. This option is only available when <i>Role</i> is <i>User</i> .

6. Select *OK* to save the setting.

#### To create a new RADIUS client:

1. Go to *Authentication > RADIUS Service > Clients*.
2. Select *Create New* from the toolbar.
3. Configure the following settings:

<b>Name</b>	Enter a name for the RADIUS client entry.
<b>Client name/IP</b>	Enter the IP address or Fully Qualified Domain Name (FQDN) of the FortiAnalyzer.
<b>Secret</b>	Enter the server secret. This value must match the FortiAnalyzer RADIUS server setting at <i>System Settings &gt; Admin &gt; Remote Auth Server</i> .
<b>First profile name</b>	See the <i>FortiAuthenticator Administration Guide</i> .
<b>Description</b>	Enter an optional description for the RADIUS client entry.
<b>Apply this profile based on RADIUS attributes</b>	Select to apply the profile based on RADIUS attributes.
<b>Authentication method</b>	Select <i>Enforce two-factor authentication</i> from the list of options.
<b>Username input format</b>	Select the username input format.
<b>Realms</b>	Configure realms.

<b>Allow MAC-based authentication</b>	Optional configuration.
<b>Check machine authentication</b>	Select to check machine based authentication and apply groups based on the success or failure of the authentication.
<b>Enable captive portal</b>	Enable various portals.
<b>EAP types</b>	Optional configuration.

4. Select *OK* to save the setting.

## Configuring FortiAnalyzer

The following instructions describes the steps required on your FortiAnalyzer device to configure two-factor authentication for administrator logins.

### To configure the RADIUS server:

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

**New RADIUS Server**

Name

Server Name/IP

Port

Server Secret

Secondary Server Name/IP

Secondary Server Secret

Authentication Type

3. Configure the following settings:

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

4. Select *OK* to save the setting.

**To create the administrator users:**

1. Go to *System Settings > Admin > Administrator*.
2. Select *Create New* from the toolbar.
3. Configure the settings, selecting the previously added RADIUS server from the *RADIUS Server* drop-down list. See [Adding a RADIUS server on page 57](#).
4. Click *OK* to save the settings.

**To test the configuration:**

1. Attempt to log into the FortiAnalyzer GUI with your new credentials.
2. Enter your user name and password then select *Login*.
3. Enter your FortiToken pin code then select *Submit* to finish logging in to FortiAnalyzer.

## Global administrator settings

The *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 GUI
- Password Policy

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

## Configuring global administrative settings

**To configure administrative settings:**

1. Go to *System Settings > Admin > Admin Settings*. For a description of the fields, see [Global Administrator Settings page on page 66](#).

**Admin Settings**

**Administration Settings**

HTTP Port: 80 ☐ Redirects to HTTPS

HTTPS Port: 443

HTTPS & Web Service Certificate: Fortinet\_Local

Idle Timeout: 480 (1-480 Minutes)

Language: Auto Detect

**Password Policy**

☒ Enable

Minimum Length: 8 (8-32 characters)

Must Contain: ☐ Uppercase Letters ☐ Lowercase Letters ☐ Numbers (0-9) ☐ Special Characters

Admin Password Expires after: 0 (days)

**Apply**

2. Configure the settings, and select *Apply*. The settings are applied to all administrator accounts.

## Changing the GUI language

The GUI supports multiple languages. The default language setting is *Auto Detect*; it uses the language configured on your management computer. If that language is not supported, the GUI defaults to English.

You can change the GUI language to English, Simplified or Traditional Chinese, Japanese, or Korean. For best results, you should select the language used by the operating system on the management computer.

### To change the GUI language:

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

## FortiAnalyzer language support

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Hebrew		✓
Hungarian		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Spanish		✓

Hebrew and Hungarian are not included in the default report languages. You can import language translation files for these languages via the command line interface using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP
address> <user name> <password> <file name>
execute sql-report import-lang <language name> <sftp> <server IP
address> <user name> <password> <file name>
execute sql-report import-lang <language name> <scp> <server IP
address> <user name> <password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP
address> <file name>
```

For more information, see the *FortiAnalyzer CLI Reference* available from the [Fortinet Document Library](#).

## Changing the idle timeout

You can specify how long an administrative connection can be idle before the administrator must log in again.

By default, the GUI disconnects administrative sessions if no activity takes place for fifteen minutes. The maximum amount of time that you can set is 480 minutes (8 hours). You should use the idle timeout to prevent someone from using the GUI from a PC that is logged in and then left unattended.

### To change the GUI idle timeout:

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

## Administrator account references

### Create Administrator page

Following is a description of the fields used to create and edit administrator accounts by navigating to *System Settings > Administrator* pane.

Field	Description
<b>User Name</b>	Enter the name that this administrator uses to log in.
<b>Comments</b>	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.
<b>Admin Type</b>	Select the type of authentication the administrator will use when logging into the FortiAnalyzer unit. Select one of: <i>LOCAL</i> , <i>RADIUS</i> , <i>LDAP</i> , <i>TACACS+</i> , or <i>PKI</i> .
<b>Server</b>	Select the <i>RADIUS</i> , <i>LDAP</i> , or <i>TACACS+</i> server, as appropriate. This option is only available if <i>Admin Type</i> is not <i>LOCAL</i> or <i>PKI</i> .
<b>Wildcard</b>	Select this option to set the password as a wildcard. This option is only available if <i>Admin Type</i> is not <i>LOCAL</i> or <i>PKI</i> .
<b>Subject</b>	If <i>Admin Type</i> is set to <i>PKI</i> , enter a description.
<b>CA</b>	If <i>Admin Type</i> is set to <i>PKI</i> , select a certificate in the drop-down list.
<b>Require two-factor authentication</b>	If <i>Admin Type</i> is set to <i>PKI</i> , you can select the check box to enforce two-factor authentication.



Field	Description
<b>New Password</b>	Enter the password. This option is not available if <i>Wildcard</i> is selected. If <i>Admin Type</i> is <i>PKI</i> , this option is only available when <i>Require two-factor authentication</i> is selection.
<b>Confirm Password</b>	Enter the password again to confirm it. This option is not available if <i>Wildcard</i> is selected. If <i>Admin Type</i> is <i>PKI</i> , this option is only available when <i>Require two-factor authentication</i> is selection.
<b>Admin Profile</b>	Select a profile from the list. The profile selected determines the administrator's access to the FortiAnalyzer unit's features. <i>Restricted_User</i> and <i>Standard_User</i> admin profiles do not have access to the <i>System Settings</i> tab. An administrator with either of these admin profiles will see a change password icon in the navigation pane.
<b>Administrative Domain</b>	Choose the ADOMs this administrator will be able to access, select <i>All ADOMS</i> , <i>All ADOMS except specified ones</i> or <i>Specify</i> . Select the remove icon to remove an ADOM. This field is available only if ADOMs are enabled. The <i>Super_User</i> profile can only be set to <i>All ADOMS</i> .
<b>Trusted Host</b>	Optionally, enter the trusted host IPv4 or IPv6 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 GUI or in the CLI. Setting trusted hosts for all of your administrators can enhance the security of your system.
<b>User Information</b>	Enter the administrator's email address and phone number.

## Create Administrator Profile page

Following is a description of the fields used to create and edit administrator profiles on the *System Settings > Profile* page.

Field	Description
<b>Profile Name</b>	Enter a name for this profile.
<b>Description</b>	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.
<b>Other Settings</b>	Select <i>None</i> , <i>Read Only</i> , or <i>Read-Write</i> access for the categories as required.

## Global Administrator Settings page

Following is a description of the fields used to set global administrator settings on the *System Settings > Admin > Admin Settings* page.

Field	Description
<b>HTTP Port</b>	Enter the TCP port to be used for administrative HTTP access. Select <i>Redirect to HTTPS</i> to redirect HTTP traffic to HTTPS.
<b>HTTPS Port</b>	Enter the TCP port to be used for administrative HTTPS access.
<b>HTTPS &amp; Web Service Server Certificate</b>	Select a certificate from the drop-down list.
<b>Idle Timeout</b>	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.
<b>Language</b>	Select a language from the drop-down list. Select either <i>English</i> , <i>Simplified Chinese</i> , <i>Traditional Chinese</i> , <i>Japanese</i> , <i>Korean</i> , or <i>Auto Detect</i> . The default value is <i>Auto Detect</i> .
<b>Password Policy</b>	Select to enable a password policy for all administrators.
<b>Minimum Length</b>	Select the minimum length for a password. The default is eight characters.
<b>Must Contain</b>	Select the types of characters that a password must contain.
<b>Admin Password Expires after</b>	Select the number of days that a password is valid for, after which time it must be changed.

# Devices

## About devices

Devices and VDOMs are added to the FortiAnalyzer unit by using the *Device Manager* pane. After the device or VDOM is successfully added and registered, the FortiAnalyzer unit starts collecting logs from the device or VDOM.

You can also configure the FortiAnalyzer unit to forward logs to another device. See [Log Forwarding on page 163](#).

## How ADOMs affect devices

When ADOMs are enabled, the *Device Manager* pane is displayed per ADOM. See also [Switching between ADOMs on page 28](#).



FortiAnalyzer does not support device groups.

---

## FortiClient EMS devices

You can add FortiClient EMS servers to FortiAnalyzer. Registered FortiClient EMS servers are added to the default FortiClient ADOM. You must enable ADOMs to work with FortiClient EMS servers in FortiAnalyzer. When you select the FortiClient ADOM and go to the *Device Manager* pane, the FortiClient EMS servers are displayed. See also [FortiClient support and ADOMs on page 43](#).



When you add a FortiClient EMS server to FortiAnalyzer, you can view log information for the FortiClient endpoints that are registered to the FortiClient EMS. If you want to view log information for FortiClient endpoints that are registered to a FortiGate device, you must view the FortiGate device. Log information for FortiClient endpoints is stored with the device to which the FortiClient endpoint is registered.

---

## Unregistered devices

In FortiAnalyzer 5.2.0 and 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 is displayed in the *Device Manager > Devices Unregistered* pane. You can then add devices to specific ADOMs or delete devices by using the toolbar buttons or right-click menu.

## Adding devices

You must add and register devices and VDOMs to the FortiAnalyzer unit to enable the device or VDOM to send logs to the FortiAnalyzer unit. Registered devices are also known as devices that have been promoted to the DVM

table.



Devices must be configured to send logs to the FortiAnalyzer unit. For example, after you add and register a FortiGate device with the FortiAnalyzer unit, you must also ensure that the FortiGate device is configured to send logs to the FortiAnalyzer unit. In the device GUI, go to *Log & Report > Log Settings*, and set the *Send Logs to FortiAnalyzer/FortiManager* setting.

## Adding devices using the wizard

You can add devices and VDOMs to FortiAnalyzer by using the *Add Device* wizard. When the wizard finishes, the device is added to the FortiAnalyzer unit, registered, and ready to start sending logs.

### To add devices by using the wizard:

1. If ADOMs are enabled, ensure you are working in the ADOM to which the device will be added. Otherwise skip this step.
2. Go to *Device Manager* and click *Add Device*.

The *Add Device* wizard is displayed. For a description of the fields in the wizard, see [Add Device wizard on page 73](#).

The screenshot shows the 'Add Device' wizard interface. It has a title bar 'Add Device' and a subtitle 'Please input the following information to add a device.' Below this are several input fields: 'IP Address' with a placeholder 'IP', 'SN' with a placeholder 'SN', 'Device Name' with a placeholder 'Name', 'Device Model' with a dropdown menu showing 'Input SN to see available versions...', 'Firmware Version' with a dropdown menu showing '5.4', and 'Description' with a placeholder 'Description'. At the bottom right are two buttons: 'Next >' (blue) and 'Cancel' (orange).

3. Fill in the fields then click *Next*.

The device will be added to the ADOM and, if successful, will be ready to begin sending logs to the FortiAnalyzer unit.

Add Device

Name	log1
SN	FGVM02Q105060031
IP Address	10.3.23.2
Status	<div><div>✔ Device Added Successfully</div><div><div>✔ Creating device database</div><div>✔ Retrieving high availability status</div><div>✔ Initializing configuration database</div><div>✔ Updating group membership</div><div>✔ Successfully add device</div></div></div>

Finish

4. Click *Finish* to close the wizard.

## Adding devices manually

Supported devices can be configured to send logs to the FortiAnalyzer device. The devices are then displayed in the root ADOM as unregistered devices. You can quickly view unregistered devices by clicking *Unregistered Devices* in the quick status bar. When you manually add an unregistered device to the FortiAnalyzer unit, the device is registered with the FortiAnalyzer unit, and FortiAnalyzer can start receiving logs from the device.

When ADOMs are enabled, you can assign the device to an ADOM.

### To manually add devices:

1. In the root ADOM, go to *Device Manager* and click *Unregistered Devices* in the quick status bar. The content pane displays the unregistered devices.
2. Select the unregistered device or devices, then click *Add*. The *Add Device* dialog box opens.
3. If ADOMs are enabled, select the ADOM in the *Add the following device(s) to ADOM* list. If ADOMs are disabled, select *root*.
4. Click *OK* to register the device or devices.

The device or devices are added, and FortiAnalyzer can start receiving logs from the device or devices.



When manually adding multiple devices at one time, they are all added to the same ADOM.

## Managing registered devices

You can manage registered devices from the *Device Manager* pane. Some options are available in the menu on the toolbar. Some options are available in the right-click menu. Right-click a device to display the menu.

Option	Description
<b>Add Device</b>	Add and register a new device to the FortiAnalyzer unit by using the <i>Add Device</i> wizard.
<b>Edit</b>	Edit the selected device.
<b>Delete</b>	Delete the selected device.
<b>Column Settings</b>	Click to select which columns to display on the <i>Device Manager</i> pane.
<b>More</b>	Click to import or export a device list.

## Using the quick status bar

You can quickly view the status of devices on the *Device Manager* pane by using the quick status bar, which contains the following information:

- Devices Total
- Devices Unregistered
- Devices Log Status Down
- Storage Used

You can also click each quick status to display in the content pane only the devices referenced in the quick status.

### To use the quick status bar:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to the *Device Manager* pane. The quick status bar is displayed. By default, the content pane displays all registered devices.



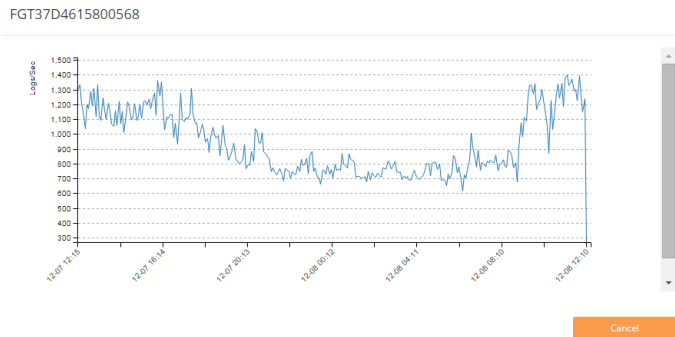
3. Click each quick status to filter the devices displayed in the content pane.  
For example, click *Devices Log Status Down*. The content pane changes to display only the devices with a log status of down.
4. Click *Devices Total* to return to the main view.

## Displaying historical average log rates

You can display a graph of the historical, average log rates for each device.

### To display historical average logs rates:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to the *Device Manager* pane. The list of devices is displayed.
3. In the *Average Log Rate (log/sec)* column, click the number. A graph is displayed.



4. Hover the mouse over the graph to display more detail.

## Managing unregistered devices

You can manage unregistered devices from the *Device Manager > Devices Unregistered* pane. Some options are available in the menu on the toolbar. Some options are available in the right-click menu. Right-click a device to display the menu.

Option	Description
<b>Add</b>	Add an unregistered device to the FortiAnalyzer unit to register the device with FortiAnalyzer. When you configure a supported device to send logs to the FortiAnalyzer unit, the device is displayed in the unregistered list until you add the device to FortiAnalyzer.
<b>Delete</b>	Delete the selected unregistered device.

## Device references

This section describes the options on the *Device Manager* pane.

### Device Manager pane > quick status bar

The *Device Manager* pane includes the following information in a quick status bar.

Quick Status	Description
<b>Devices Total</b>	Displays the registered devices. Click the quick status to display all registered devices in the content pane.
<b>Devices Unregistered</b>	Displays the unregistered devices. Click the quick status to display only unregistered devices in the content pane.

Quick Status	Description
<b>Devices Log Status Down</b>	Displays the log status for registered devices. Click the quick status to display only devices with a log status of down in the content pane.
<b>Storage Used</b>	Displays the <i>FortiView &gt; Summary &gt; System &gt; Storage Statistics</i> page.

## Device Manager > Devices Total pane

The following columns are displayed on the *Device Manager > Devices Total* and the *Device Manager > Devices Log Status Down* pane.

Column	Description
<b>Device Name</b>	Displays the name of the device.
<b>IP Address</b>	Displays the IP address for the device.
<b>Platform</b>	Displays the platform for the device.
<b>Logs</b>	Identifies whether the device is successfully sending logs to the FortiAnalyzer unit. A green circle indicates that logs are being sent. A red circle indicates that logs are not being sent. A lock icon displays when a secure tunnel is being used to transfer logs from the device to the FortiAnalyzer unit.
<b>Average Log Rate (log/sec)</b>	Displays the average rate at which the device is sending logs to the FortiAnalyzer unit in log rate per second. Click the number to display a graph of historical average log rates.
<b>Device Storage</b>	Displays how much of the allotted disk space has been consumed by logs.
<b>Description</b>	Displays a description of the device.

The following buttons and menus are available for selection on the toolbar:

Button	Description
<b>Add Device</b>	Opens the <i>Add Device Wizard</i> to add a device to the FortiAnalyzer unit. The device is added, but not registered with the FortiAnalyzer unit. Unregistered devices are displayed in the <i>Unregistered Devices</i> tree menu.
<b>Edit</b>	Edit the selected device.
<b>Delete</b>	Click to deleted the selected device from the FortiAnalyzer unit.



Button	Description
<b>Column Settings</b>	Click the <i>Column Settings</i> menu, and select the columns that you want to display in the content pane. Select <i>Reset to Default</i> to display the default columns.
<b>More</b>	Click the <i>More</i> menu, and select <i>Import Device List</i> or <i>Export Device List</i> .
<b>Search</b>	Type the name of a device. The content pane displays the results. Clear the search box to display all devices in the content pane.

## Device Manager > Unregistered Devices pane

The following columns are displayed on the *Device Manager > Unregistered Devices* pane.

Column	Description
<b>Device Name</b>	Displays the name of the device.
<b>Model</b>	Displays the model of the device.
<b>Serial Number</b>	Displays the serial number for the device.
<b>Connecting IP</b>	Displays the IP address for the device

The following buttons and menus are available for selection on the toolbar:

Button	Description
<b>Add</b>	Click to register the selected device with the FortiAnalyzer unit, which enables the FortiAnalyzer unit to receive logs from the device.
<b>Delete</b>	Click to deleted the selected device from the FortiAnalyzer unit.

## Add Device wizard

Following is a description of the fields in the *Add Device* wizard.

Field	Description
<b>IP Address</b>	Type the IP address for the device.
<b>SN</b>	Type the serial number for the device.
<b>Device Name</b>	Type a name for the device.
<b>Device Model</b>	Select the model of the device.

Field	Description
<b>Firmware Version</b>	Select the firmware version of the device.
<b>Description</b>	Type a description of the device (optional).
<b>Next</b>	Click to proceed to the next screen.
<b>Cancel</b>	Click to cancel the wizard.

## Edit Device pane

Following is a description of the fields in the *Edit Devices* pane.

Field	Description
<b>Name</b>	Displays the name of the device added to the FortiAnalyzer unit.
<b>Description</b>	Displays a description of the device.
<b>Company/Organization</b>	Displays the name of the company or organization that owns the device.
<b>Country</b>	Displays the name of the country where the device resides.
<b>Province/State</b>	Displays the name of the province or state where the device resides.
<b>City</b>	Displays the name of the city where the device resides.
<b>Contact</b>	Displays the contact information for the device.
<b>Geographic Coordinates</b>	This section displays the latitude and longitude coordinates for the device.
<b>Latitude</b>	Displays the latitude of the device location to support the interactive map on the <i>FortiView &gt; Summary &gt; Threats &gt; Threat Map</i> pane.
<b>Longitude</b>	Displays the longitude of the device location to support the interactive map on the <i>FortiView &gt; Summary &gt; Threats &gt; Threat Map</i> pane.
<b>IP Address</b>	Displays the IP address for the device.
<b>Admin User</b>	Displays the admin login for the device.
<b>Password</b>	Displays the password for the admin login.
<b>Device Information</b>	This section displays the serial number, device model, and firmware version for the device.
<b>Serial Number</b>	Displays the serial number for the device.

Field	Description
<b>Device Model</b>	Displays the model of the device
<b>Firmware Version</b>	Displays the firmware version of the device.
<b>HA Cluster</b>	Displays whether the device is part of a high-availability pair. Select to identify the device as part of an HA pair, and then identify the other device in the HA pair.
<b>Secure Connection</b>	Select to enable a secure connection between the device and the FortiAnalyzer unit.
<b>ID</b>	Displays the ID for the device.
<b>Pre-Shared Key</b>	Enter the pre-shared key for the device.
<b>Device Permissions</b>	Specify the permission for the device.

# Log and File Storage

## About log and file storage

Logs and files are stored on the FortiAnalyzer disks. Logs are also temporarily stored in the SQL database.

You can configure data policy and disk utilization settings for devices, which are collectively called log storage settings.

You can also configure global log and file storage settings, which apply to all logs and files in the FortiAnalyzer system regardless of log storage settings.

## How ADOMs affect log storage

ADOMs affect the log storage settings as follows:

- When ADOMs are enabled, you can configure unique log storage settings for each ADOM, and the settings apply to all devices in each ADOM.
- When ADOMs are disabled, you can configure log storage settings once, and the settings apply to all managed devices.



You can also configure global log settings by using the *System Settings > Advanced > File Management* pane. The settings apply to all logs on the FortiAnalyzer unit in addition to the log storage settings.

## FortiAnalyzer disk space allocation

In FortiAnalyzer, the system reserves 5% to 25% disk space for system usage and unexpected quota overflow. Only 75% to 95% disk space is available for allocation to devices.

Reports are stored in the reserved space.

Disk Size	Reserved Disk Quota
<b>Small Disk (less than 500GB)</b>	The system reserves either 20% or 50GB of disk space, which ever is smaller.
<b>Medium Disk (less than 1000GB)</b>	The system reserves either 15% or 100GB of disk space, which ever is smaller.
<b>Large Disk (less than 3000GB)</b>	The system reserves either 10% or 200GB of disk space, which ever is smaller.
<b>Very Large Disk (less than 5000GB)</b>	The system reserves either 5% or 500GB of disk space, which ever is smaller.

**Disk Size****Reserved Disk Quota**

**Note:** The RAID level selected will impact the determination of the disk size and reserved disk quota level. For example, a FAZ-1000C with four 1TB hard drives configured in RAID 10 will be considered a large disk and 10% or 200GB disk space will be reserved.

## Disk fullness and automatic log deletion

When compressed logs from devices fill up the allotted FortiAnalyzer disk space to a specified threshold, the following actions take place for the logs:

- An alert message is generated
- The oldest compressed logs are deleted for the device

The allotted disk space is defined by the log storage settings.

You can also specify a global automatic deletion policy for all logs on the FortiAnalyzer unit by using settings on the *System Settings > Advanced > File Management* pane. Both global settings and log storage settings are active at all times.

## Automatic deletion of logs and files

Logs and files are automatically deleted from the FortiAnalyzer unit by using the following policies:

- Global automatic file deletion  
The global automatic deletion policy specifies when to delete the oldest compressed logs, quarantined files, reports, and archived files from the FortiAnalyzer disks, regardless of the associated log storage settings. You can specify the settings on the *System Settings > Advanced > File Management* pane.
- Data policy  
The data policy specifies how long to store compressed logs for each device. When the specified amount of time expires, compressed logs for the device are automatically deleted from the FortiAnalyzer disks. Deletion of logs is triggered by the data policy associated with the device.
- Disk fullness automatic deletion policy  
The disk fullness and automatic deletion policy automatically deletes the oldest compressed logs for each device from the FortiAnalyzer disks when the allotted disk space becomes full. The allotted disk space is defined by the log storage settings. Alerts to warn you when the allotted disk space is getting full.

All deletion policies are active on the FortiAnalyzer unit at all times, and you should carefully configure each policy. For example, if the disk fullness policy for a device hits its threshold before the global automatic file deletion policy for the FortiAnalyzer unit, compressed logs for the affected device are automatically deleted. Conversely, if the global automatic file deletion policy hits its threshold first, the oldest compressed logs on the FortiAnalyzer unit, regardless of the log storage settings associated with the device, are automatically deleted.

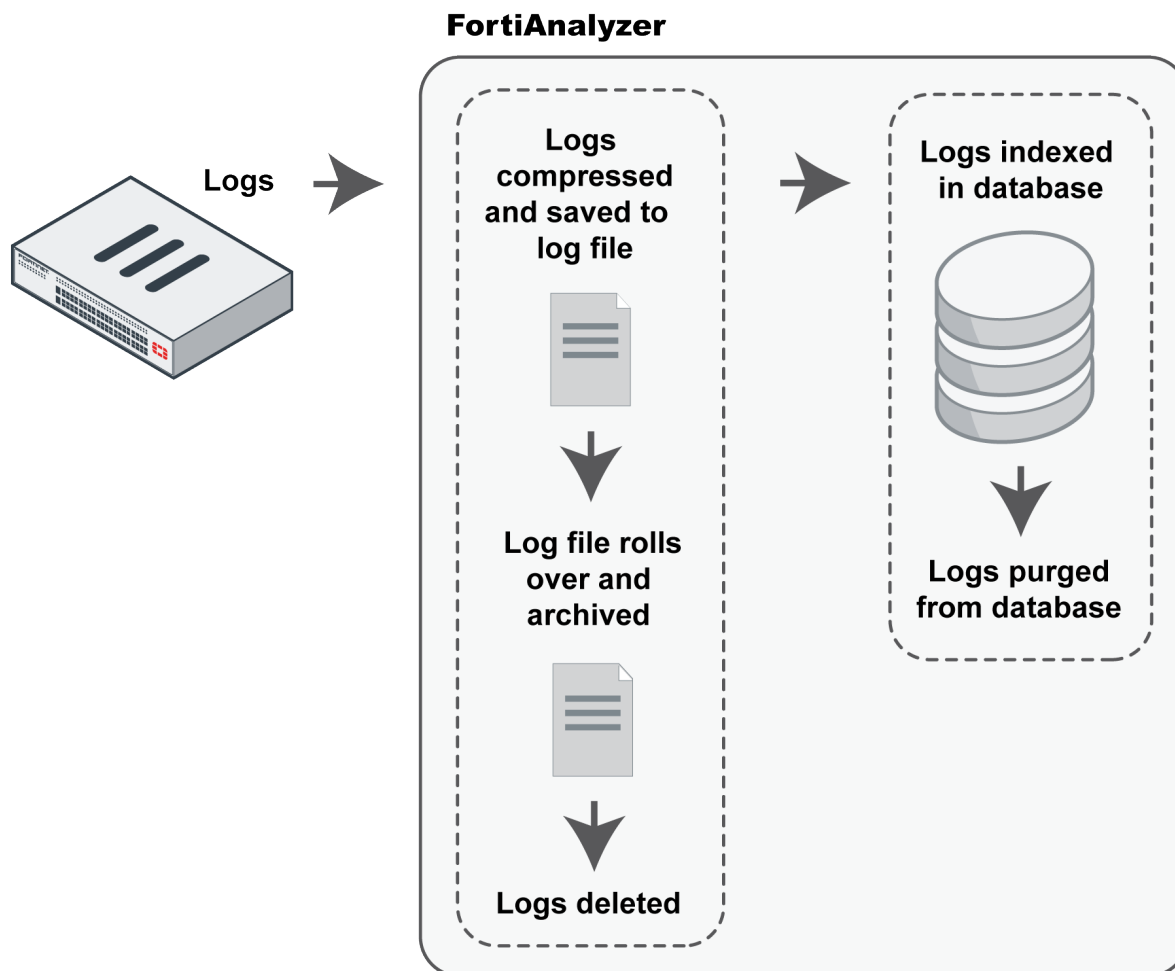
The following table summarizes the different automatic deletion policies:

Policy	Scope	Trigger
Global automatic file deletion	All logs, files, and reports on the system	When the specified amount of time expires, old files are automatically deleted. This policy affects all files in the system regardless of the data policy settings associated with devices.
Data policy	Logs for the device with which the data policy is associated	When the specified amount of retention time expires, old compressed logs for the device are deleted. This policy affects only compressed logs for the device with which the data policy is associated.
Automatic log deletion	Logs for the device with which the log storage settings are associated	When the specified threshold is reached for the allotted amount of disk space for the device, the oldest compressed logs are deleted for the device. This policy affects only compressed logs for the device with which the log storage settings are associated.

## FortiAnalyzer log files for storing logs

When devices send logs to a FortiAnalyzer unit, the logs are compressed and saved in a log file on the FortiAnalyzer disks. When the log file reaches the specified size threshold, the log file rolls over, and a new log file is created to receive the incoming logs. You can specify the size at which the log file rolls over. You can specify the settings on the *System Settings > Advanced > Device Log Settings* pane.

## Log and file workflow



When devices send logs to a FortiAnalyzer unit, the logs enter the following automatic workflow:

1. Logs are compressed and saved in a log file on the FortiAnalyzer disks.  
When the log file that receives new logs reaches a specific size, it rolls over and is archived. A new log file is created to receive incoming logs. You can specify the size at which the log file rolls over.
2. Logs are indexed in the SQL database to support analysis.  
You can specify how long to keep logs indexed by using a data policy.
3. Logs are purged from the SQL database, but remain compressed in a log file on the FortiAnalyzer disks.
4. Logs are deleted from the FortiAnalyzer disks.  
You can specify how long to keep logs by using a data policy.

While logs are indexed in the SQL database, they are considered online, and you can view details about the logs on the *FortiView* pane and the *Event Monitor* pane. You can also generate reports about the logs by using the *Reports* pane.

While logs are compressed and stored on the FortiAnalyzer disks, they are considered offline, and you cannot immediately view details about the logs on the *FortiView* pane or the *Event Monitor* pane. You also cannot immediately generate reports about the logs by using the *Reports* pane. For more information, see [Compressed logs and indexed logs on page 20](#).

The following table summarizes the differences between indexed and compressed log phases:

Log Phase	FortiAnalyzer Location	Immediate Analytic Support
Indexed	Compressed in log file and indexed in SQL database	Yes. You can view details about the logs on the <i>FortiView</i> pane and the <i>Event Monitor</i> pane. You can also generate reports about the logs on the <i>Reports</i> pane.
Compressed	Compressed in log file	No. You cannot immediately view details about the logs on the <i>FortiView</i> pane or the <i>Event Monitor</i> pane. You also cannot generate reports about the logs by using the <i>Reports</i> pane. To view details about the logs again, see Log fetcher management on page 1.

You can control how long logs remain indexed and compressed by using a data policy. See [Configuring log storage on page 80](#).

## Configuring log storage

You can use a data policy and disk utilization settings to control log storage. See also [How ADOMs affect log storage on page 76](#).

### Configuring log storage settings

When ADOMs are enabled, you can configure log storage settings for each ADOM, and the settings apply to all devices in each ADOM. You can specify the settings when you create or edit an ADOM or by using the *Storage Info* pane.

When ADOMs are disabled, you can configure log storage settings once on the *System Settings > Dashboard* pane, and the settings apply to all managed devices.

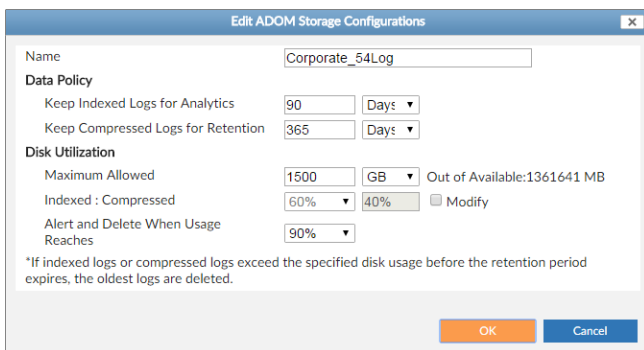


The log storage settings affect only the logs and SQL database for the device with which the log storage settings are associated. Reports are not affected. See [FortiAnalyzer disk space allocation on page 76](#).

#### To configure log storage settings with ADOMs enabled:

1. Go to *System Settings > Storage Info*.
2. Select an ADOM, and click *Edit*. The *Edit ADOM Storage Configurations* dialog box is displayed.





**Edit ADOM Storage Configurations**

Name: Corporate\_54Log

**Data Policy**

Keep Indexed Logs for Analytics: 90 Days

Keep Compressed Logs for Retention: 365 Days

**Disk Utilization**

Maximum Allowed: 1500 GB Out of Available: 1361641 MB

Indexed : Compressed: 60% 40% ☐ Modify

Alert and Delete When Usage Reaches: 90%

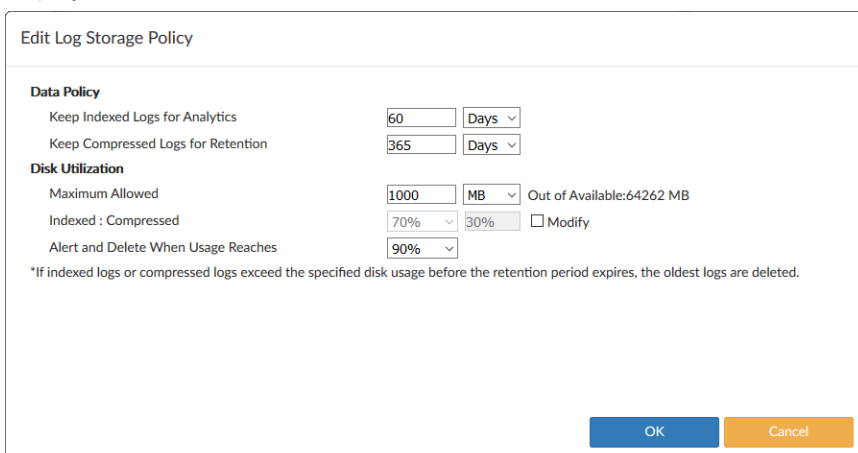
\*If indexed logs or compressed logs exceed the specified disk usage before the retention period expires, the oldest logs are deleted.

OK Cancel

3. Configure the settings, and click **OK**. For a description of the options, see [Edit ADOM Storage Configuration dialog box on page 89](#).

### To configure log storage settings with ADOMs disabled:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, click *Edit Log Storage Policy*. The *Edit Log Storage Policy* dialog box is displayed.



**Edit Log Storage Policy**

**Data Policy**

Keep Indexed Logs for Analytics: 60 Days

Keep Compressed Logs for Retention: 365 Days

**Disk Utilization**

Maximum Allowed: 1000 MB Out of Available: 64262 MB

Indexed : Compressed: 70% 30% ☐ Modify

Alert and Delete When Usage Reaches: 90%

\*If indexed logs or compressed logs exceed the specified disk usage before the retention period expires, the oldest logs are deleted.

OK Cancel

3. Configure the settings, and click **OK**. For a description of the options, see [Edit ADOM Storage Configuration dialog box on page 89](#).

## Editing log storage settings

When ADOMs are enabled, you can edit log storage settings for each ADOM. The log storage settings apply to all devices in the ADOM.

When ADOMs are disabled, you can edit logs storage settings once, and the log storage settings apply to all managed devices.



If you change the log storage settings, the new date ranges affect indexed and compressed logs that are currently on the FortiAnalyzer unit. Depending on the date change, indexed files can be purged from the database, compressed files can be added back to the database, and compressed logs outside the date range can be deleted.

**To change log storage settings with ADOMs enabled:**

1. Go to *System Settings > Storage Info*.
2. Select an ADOM, and click *Edit*.
3. Change the settings, and select *OK*. For a description of the options, see [Edit ADOM Storage Configuration dialog box on page 89](#).

**To change log storage settings with ADOMs disabled:**

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, click *Edit Log Storage Policy*. The *Edit Log Storage Policy* dialog box is displayed.
3. Change the settings, and select *OK*. For a description of the options, see [Edit ADOM Storage Configuration dialog box on page 89](#).

## Monitoring log storage capacity

You can monitor FortiAnalyzer disk space consumption. You can also monitor disk usage for each device. See [Monitoring disk usage for devices on page 138](#).

**To monitor log storage capacity with ADOMs enabled:**

1. Go to *System Settings > Storage Info*. For a description of the page, see [Storage Info pane on page 88](#).
2. Go to *Device Manager > Storage Used*. For a description of the page, see [Viewing log storage statistics on page 138](#).

You can also access this page by going to *FortiView > System > Storage Statistics*.

**To monitor log storage capacity with ADOMs disabled:**

1. Go to *Device Manager > Storage Used*. For a description of the page, see [Viewing log storage statistics on page 138](#).

You can also access this page by going to *FortiView > System > Storage Statistics*.

## Managing log storage settings

When ADOMs are enabled, you can manage log storage settings from the *System Settings > Storage Info* pane. Some options are available in the menu on the toolbar. Some options are available in the right-click menu. Right-click an ADOM or device to display the menu.



When ADOMs are disabled, you can manage log storage settings from the *System Settings > Dashboard > System Information* widget.

Option	Description
<b>Edit</b>	Edit the log storage settings.
<b>Refresh</b>	Refresh the storage information for the <i>System Settings &gt; Storage Info</i> pane.

## Configuring global log and file settings

### Configuring global automatic deletion

FortiAnalyzer allows you to configure automatic deletion of compressed logs, quarantined files, reports, and content archive files after a set period of time. These settings are active in addition to the log storage settings. See [Automatic deletion of logs and files on page 77](#) and [Data policy and automatic deletion on page 21](#).

**To configure global automatic deletion settings:**

1. Go to *System Settings > Advanced > File Management*.
2. Configure the following settings, and select *Apply*.

<b>Device log files older than</b>	Select to enable automatic deletion of compressed log files. Enter a value in the text field, then select the time period from the drop-down list ( <i>Hours, Days, Weeks, or Months</i> ). See also <a href="#">Compressed logs and indexed logs on page 20</a> .
<b>Quarantined files older than</b>	Select to enable automatic deletion of quarantined, compressed log files. Enter a value in the text field, and select the time period from the drop-down list.
<b>Reports older than</b>	Select to enable automatic deletion of reports of data from compressed log files. Enter a value in the text field, and select the time period from the drop-down list.
<b>Content archive files older than</b>	Select to enable automatic deletion of IPS and DP archives from compressed logs. Enter a value in the text field, and select the time period from the drop-down list.

### Configuring rolling and uploading of logs

The device log settings menu allows you to configure event logging, log rollover, and upload options. The device log settings are global and apply to all logs on the FortiAnalyzer unit.

**To configure device log settings:**

1. Go to *System Settings > Advanced > Device Log Settings*. The *Device Log Settings* pane is displayed.

Device Log Settings

**Registered Device Logs**

Roll log file when size exceeds  (10-500)MB

☒ Roll log files at scheduled time

Hour  Minute

☒ Upload logs using a standard file transfer protocol

Upload Server Type

Upload Server IP

User Name

Password

Remote Directory

Upload Log Files ☒ When rolled ☐ Daily at  Hour

☐ Upload log files in gzip file format

☐ Delete log files after uploading

**Local Device Log**

☒ Send the local event logs to FortiAnalyzer/FortiManager

IP Address

Upload Option ☒ Real-time ☐ Schedule Time

Severity Level

☐ Secure connection for log transmission

[Apply](#)

2. Configure the following settings, then click *Apply*:

Registered Device Logs	
<b>Roll log file when size exceeds</b>	Enter the log file size. Range: 10 to 500 MB
<b>Roll log files at a scheduled time</b>	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.
<b>Upload logs using a standard file transfer protocol</b>	Select to upload logs and configure the following settings.
<b>Upload Server Type</b>	Select one of <i>FTP</i> , <i>SFTP</i> , or <i>SCP</i> .
<b>Upload Server IP</b>	Enter the IP address of the upload server.
<b>User Name</b>	Select the username that will be used to connect to the upload server.
<b>Password</b>	Select the password that will be used to connect to the upload server.
<b>Remote Directory</b>	Select the remote directory on the upload server where the log will be uploaded.
<b>Upload Log Files</b>	Select to upload log files when they are rolled according to settings selected under <i>Roll Logs</i> or daily at a specific hour.

<b>Upload log files in gzip format</b>	Select to gzip the logs before uploading. This will result in smaller logs, and faster upload times.
<b>Delete log files after uploading</b>	Select to remove device log files from the FortiAnalyzer system after they have been uploaded to the Upload Server.
<b>Local Device Log</b>	
<b>Send the local event logs to FortiAnalyzer / FortiManager</b>	Select to send local event logs to another FortiAnalyzer or FortiManager device.
<b>IP Address</b>	Enter the IP address of the FortiAnalyzer or FortiManager.
<b>Upload Option</b>	Select to upload logs realtime or at a scheduled time. When selecting a scheduled time, you can specify the hour and minute to upload logs
<b>Severity Level</b>	Select the minimum log severity level from the drop-down list.
<b>Secure connection for log transmission</b>	Select to use a secure connection for log transmission.

## Configuring rolling and uploading of logs by using the CLI

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 GUI, they are in the following format:

```
FG3K6A3406600001-tlog.1252929496.log-2012-09-29-08-03-54.gz
```

If you have enabled log uploading, you can choose to automatically delete the rolled log file after uploading, thereby freeing the amount of disk space used by rolled log files. If the log upload fails, such as when the FTP server is unavailable, the logs are uploaded during the next scheduled upload.

Log rolling and uploading can be enabled and configured in the GUI in *System Settings > Advanced > Device Log Settings*. For more information, see [Configuring rolling and uploading of logs on page 83](#). Log rolling and uploading can also be enabled and configured using the CLI. For more information, see the [FortiAnalyzer CLI Reference](#).

**To enable or disable log file uploads:**

To enable log uploads, enter the following CLI commands:

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

To disable log uploads, enter the following CLI commands:

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

**To roll logs when they reach a specific size:**

Enter the following CLI commands:

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

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

**To roll logs on a schedule:**

To disable log rolling, enter the following CLI commands:

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

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

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

## Managing logs

You can manage logs by using storage info settings and by using system settings. You can also monitor logs by using a number of different options.

Option	Description
When ADOMs are enabled, specify how long an ADOM should store compressed logs and keep logs indexed in the SQL database for its devices.	Go to <i>System Settings &gt; Storage Info</i> and edit an entry.
When ADOMs are disabled, specify how long to store compressed logs and keep logs indexed in the SQL database for all managed devices.	Go to <i>System Setting &gt; Dashboard &gt; System Information</i> , and edit the <i>Log Storage Policy</i> .
When ADOMs are enabled, specify how much disk space each ADOM should use for its logs.	Go to <i>System Settings &gt; Storage Info</i> and edit an entry.
When ADOMs are disabled, specify how much disk space to use for logs for all managed devices.	Go to <i>System Setting &gt; Dashboard &gt; System Information</i> , and edit the <i>Log Storage Policy</i> .
When ADOMs are enabled, specify at what fullness threshold each ADOM should automatically delete the oldest compressed logs for its devices.	Go to <i>System Settings &gt; Storage Info</i> and edit an entry.
When ADOMs are disabled, specify at what fullness threshold the oldest compressed logs for all devices should be deleted.	Go to <i>System Setting &gt; Dashboard &gt; System Information</i> , and edit the <i>Log Storage Policy</i> .

Option	Description
Create a global policy to automatically delete logs regardless device.	Go to <i>System Settings &gt; Advanced &gt; File Management</i> .
When ADOMs are enabled, monitor how much disk space logs have consumed.	Go to <i>System Settings &gt; Storage Info</i> .
Monitor how much disk space logs have consumed.	Go to <i>Device Manager &gt; Storage Used</i> or <i>FortiView &gt; Summary &gt; System &gt; Storage Statistics</i> .
View analysis of indexed logs	Go to <i>FortiView</i> .
View indexed and compressed logs	Go to <i>Log View</i> .

## Log storage references

### Storage Info pane

Following is a description of the options available on the *System Settings > Storage Info* page.

Field	Description
<b>Name</b>	Displays the name of the ADOM. ADOMs are listed in the following groups: <i>FortiGates and FortiCarriers</i> and <i>Other Device Types</i> . You can expand and hide the groups to view the ADOMs contained in the group.
<b>Analytics (Actual/Config Days)</b>	Displays how long device logs for the ADOM will be indexed in the SQL database to support analysis. When device logs are indexed in the database, you can view information about the logs on the <i>FortiView</i> tab, <i>Event Monitor</i> tab, and <i>Reports</i> tab. When the time for the analytic policy expires, the device logs are automatically purged from the database and retained as compressed logs for the duration of the <i>Retention Policy</i> .
<b>Archive (Actual/Config Days)</b>	Displays how long device logs for the ADOM will be stored offline in a compressed format. When device logs are compressed, they are not indexed in the database. As a result, you cannot view information about the logs on the <i>FortiView</i> tab, <i>Event Monitor</i> tab, and <i>Reports</i> tab. When the time for the retention policy expires, the device logs are automatically deleted from the FortiAnalyzer unit.
<b>Max Storage</b>	Displays the maximum amount of FortiAnalyzer disk space that is allotted to store device logs in indexed and compressed formats. For more info about the maximum available space for each FortiAnalyzer unit, see <a href="#">FortiAnalyzer disk space allocation on page 76</a> .



Field	Description
<b>Analytic Usage (Used/Max)</b>	Displays how much of the maximum allotted FortiAnalyzer disk space is consumed and available for indexed logs
<b>Archive Usage (Used/Max)</b>	Displays how much of the maximum allotted FortiAnalyzer disk space is consumed and available for compressed logs

## Edit ADOM Storage Configuration dialog box

Following is a description of the options available on the *Edit ADOM Storage Configurations* dialog box.

When ADOMs are disabled, you can access the options on the *System Settings > Dashboard > System Information* widget.

Field	Description
<b>Name</b>	Displays the name of the selected ADOM. Type a new name to create a new ADOM.
<b>Data Policy</b>	Use the <i>Data Policy</i> settings to specify how long to keep logs in the indexed and compressed states.
<b>Keep Indexed Logs for Analytics</b>	Specify how long to keep logs in the indexed state. During the indexed state, logs are indexed in the SQL database for the specified amount of time, and you can view information about the logs on the <i>FortiView</i> , <i>Event Monitor</i> , and <i>Reports</i> tabs. After the specified amount of time expires, logs are automatically purged from the SQL database.
<b>Keep Compressed Logs for Retention</b>	Specify how long to keep logs in the compressed state. During the compressed state, logs are stored in a compressed format on the FortiAnalyzer unit. When logs are in the compressed state, you cannot view information about the log messages on the <i>FortiView</i> , <i>Event Monitor</i> , and <i>Reports</i> tabs. After the specified amount of time expires, compressed logs are automatically deleted from the FortiAnalyzer unit.
<b>Disk Utilization</b>	Use the <i>Disk Utilization</i> settings to specify how much FortiAnalyzer disk space to use for logs.
<b>Maximum Allowed</b>	Specify a maximum amount of FortiAnalyzer disk space to use for logs, and select the unit of measure. You can view the total available space for the FortiAnalyzer unit. For more info about the maximum available space for each FortiAnalyzer unit, see <a href="#">FortiAnalyzer disk space allocation on page 76</a> .

Field	Description
<b>Indexed: Compressed</b>	Specify how much of the allotted space to use for indexed and compressed logs. Indexed logs require more space than compressed logs. For example, a setting of 70% and 30% indicates that 70% of the allotted disk space will be used indexed logs, and 30% of the allotted space will be used for compressed logs. Select the <i>Modify</i> check box to change the setting.
<b>Alert and Delete When Usage Reaches</b>	Specify at what fullness you want alert messages to be generated and compressed logs to be automatically deleted. The oldest compressed logs are deleted first.

# Reports

## About reports

You can generate reports of data from logs by using *Reports*. You can use predefined reports. You can also create customize reports. Predefined report templates, charts, and macros are available to help you create new reports.

Report files are stored in the reserved space for the FortiAnalyzer device. See [Disk fullness and automatic log deletion on page 77](#).



When rebuilding the SQL database, Reports will not be available until after the rebuild is completed. Select the *Show Progress* link in the message to view the status of the SQL rebuild.

## How ADOMs affect reports

When ADOMs are enabled, each ADOM has its own reports, libraries, and advanced settings. Make sure that you are in the correct ADOM before selecting a report. See also [Switching between ADOMs on page 28](#).

Some reports are available only when ADOMs are enabled. For example, ADOMs must be enabled to access reports for FortiCarrier, FortiCache, FortiClient, FortiDDoS, FortiMail, FortiSandbox, and FortiWeb devices. You can configure and generate reports for these devices within their respective, default ADOM. These devices also have device-specific charts and datasets.

## Predefined reports, templates, charts, and macros

FortiAnalyzer includes a number of predefined elements that you can use to create and/or build reports.

Predefined...	GUI Location	Purpose
Reports	<i>Reports &gt; Report Definitions &gt; All Reports</i>	Available for you to generate reports directly or with minimum setting configurations. Predefined reports are actually report templates with basic, default setting configurations.
Report templates	<i>Reports &gt; Report Definitions &gt; Templates</i>	Available for you to use directly or build upon. Report templates include charts and/or macros and specify the layout of the report. A template populates the <i>Layout</i> tab of a report that is to be created. See <a href="#">List of report templates on page 111</a> .

Predefined...	GUI Location	Purpose
Charts	<i>Reports &gt; Report Definitions &gt; Chart Library</i>	Available for you to use directly or build upon, in a report template that you are creating, or in the <i>Layout</i> tab of a report that you are creating. Charts specify what data to extract from logs.
Macros	<i>Reports &gt; Report Definitions &gt; Macro Library</i>	Available for you to use directly or build upon, in a report template that you are creating, or in the <i>Layout</i> tab of a report that you are creating. Macros specify what data to extract from logs.

## Logs used for reports

*Reports* uses indexed logs to generate reports. Compressed logs are not used to generate reports. For more information, see [Data policy and automatic deletion on page 21](#).

## How charts and macros extract data from logs

Reports include charts and/or macros. Each chart and macro is associated with a dataset. When you generate a report, the dataset associated with each chart and macro extracts data from the logs and populates the charts and macros.

FortiAnalyzer includes a number of predefined charts and macros. You can also create custom charts and macros.

## How auto-cache works

When you generate a report, it can take days to assemble the required dataset and produce the report, depending on the required datasets. Instead of assembling datasets at the time of report generation, you can enable the *auto-cache* feature for the report.

Auto-cache is a setting that tells the system to automatically generate *hcache*. Hcache stands for "hard cache", which means the cache stays on disk in the form of database tables instead of memory. Hcache is applied to "matured" database tables. When a database table rolls, it becomes "mature", meaning the table will not grow anymore. Therefore, it is unnecessary to query this database table each time the same SQL query comes. This is when hcache comes into play. Hcache runs queries on matured database tables in advance and caches the interim results of each query. When it is time to generate the report, much of the datasets are already assembled, and the system only needs to merge the results from hcache. This reduces report generation time significantly.

However, the auto-cache process uses system resources to assemble and cache the datasets. Also, it takes extra space to save the query results. You should only enable auto-cache for reports that require a long time to assemble datasets.

## Generating reports

### Generating reports

You can generate reports by using one of the predefined reports or by using a custom report that you created. You can find all the predefined reports and custom reports listed in *Reports > Report Definitions > All Reports*.

#### To generate a report:

1. Go to *Reports > Report Definitions > All Reports*.
2. In the content pane, select a report from the list.
3. (Optional) Click *Edit* in the toolbar and edit settings on the *Settings* and *Layout* tabs. For a description of the fields in the *Settings* and *Layout* tabs, see [Reports Settings tab on page 113](#) and [Creating charts on page 100](#) and [Creating macros on page 104](#).
4. In the toolbar of the *View Report* tab, click *Run Report*.

### Viewing completed reports

After you generate reports, you can view completed reports in the following formats: HTML, PDF, XML, and CSV.

#### To view completed reports:

1. Go to *Reports > Report Definitions > All Reports*.
2. On the report list, double-click the report to open it.
3. In the *View Report* tab, go to the instance of the report that you just generated, and click on the format in which you want to view the report to open the report in that format.

For example, if you want to review the report in HTML format, click the *HTML* link.

### Enabling auto-cache

You can enable auto-cache to reduce report generation time for reports that require a long time to assemble datasets. For information about auto-cache and hcache, see [How auto-cache works on page 92](#).

#### To enable auto-cache:

1. Go to *Reports > Report Definitions > All Reports*.
2. Select the report from the list, and click *Edit* in the tool bar.
3. In the *Settings* tab, select the *Enable Auto-cache* check box.
4. Click *OK*.

### Scheduling reports

You can configure a report to generate on a regular schedule.

**To schedule a report:**

1. Go to *Reports > Report Definitions > All Reports*.
2. Select the report from the list, and click *Edit* in the tool bar.
3. On the *Settings* tab, select the *Enable Schedule* check box and configure the schedule.
4. Click *OK*.

## Creating reports

You can create reports from report templates, by cloning and editing predefined/existing reports, or start from scratch.

### Creating reports from report templates

You can create a new report from a template. The template populates the *Layout* tab of the report. The template specifies what text, charts, and macros to use in the report and the layout of the content. Report templates do not contain any data. Data is added to the report when you generate the report.

**To create a new report from a template:**

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Report Definitions > All Reports*.
3. In the toolbar of the content pane, click *Create New*. The *Create New Report* dialog box opens.
4. Set the following options, and click *OK*:
  - a. In the *Name* box, type a name for the new report.
  - b. Select *From Template* for the *Create from* setting, and select a template from the drop-down list. The template populates the *Layout* tab for the report.
5. On the *Settings* tab, configure the settings. For a description of the fields, see [Reports Settings tab on page 113](#).
6. (Optional) On the *Layout* tab, you can tweak settings to customize the template. For a description of the fields, see [Reports Layouts tab on page 115](#).
7. Click *OK*.

### Creating reports by cloning and editing

You can create reports by cloning and editing predefined and/or existing reports.

**To create a report by cloning and editing:**

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Report Definitions > All Reports*.
3. In the content pane, select the report from the list, and click *Clone* in the tool bar.
4. In the *Clone Report* dialog box, type a name for the cloned report.
5. Edit settings on the *Settings* tab. For a description of the fields, see [Reports Settings tab on page 113](#).
6. Editing settings on the *Layout* tab. For a description of the fields, see [Reports Layouts tab on page 115](#).
7. Click *OK*.

## Creating reports without using a template

### To create a report without using a template:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Report Definitions > All Reports*.
3. In the toolbar of the content pane, click *Create New*. The *Create New Report* dialog box opens.
4. Set the following options, and click *OK*.
  - a. In the *Name* box, type a name for the new report.
  - b. Select the *Blank* option for the *Create from* setting.
5. On the *Settings* tab, you can specify a time period for the report, what device logs to include in the report, and so on. You can also add filters to the report, add a cover page to the report, and so on. For a description of the fields, see [Reports Settings tab on page 113](#).



To create a custom cover page, you must select *Print Cover Page* in the *Advanced Settings* menu.

---

6. On the *Layout* tab, you can specify the charts and macros to include in the report, as well as report content and layout.  
For a description of the fields, see [Reports Layouts tab on page 115](#). For information about creating charts and macros, see [Creating charts on page 100](#) and [Creating macros on page 104](#).
7. Click *OK*.

## Customizing report cover pages

A report cover page is only included in the report when enabled in the *Settings* tab.

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

### To customize cover page settings:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Report Definitions > All Reports*.
3. In the content pane, select the report from the list, and click *Edit* in the tool bar.
4. In the Advanced Settings section in the *Settings* tab, select the *Print Cover Page* check box, and click *Customize* next to the *Print Cover Page* option. The *Cover Page Settings* page opens.

5. Configure the following settings:

<b>Background Image</b>	Select <i>Choose</i> to open the <i>Choose a graphic</i> dialog box. Select an image, or select <i>Upload</i> to find an image on the management computer, then select <i>OK</i> to add the image as the background image of the cover page.
<b>Top Image</b>	Select <i>Choose</i> to open the <i>Choose a graphic</i> dialog box. Select an image, or select <i>Upload</i> to find an image on the management computer, then select <i>OK</i> to add the image at the top of the cover page.
<b>Top Image Position</b>	Select the top image position from the drop-down menu. Select one of the following: <i>Right</i> , <i>Center</i> , <i>Left</i> .
<b>Text Color</b>	Select the text color from the drop-down menu. Select one of the following: <i>Black</i> , <i>Bold Blue</i> , <i>Blue</i> , <i>Turquoise</i> , <i>Green</i> , <i>Bold Green</i> , <i>Yellow</i> , <i>Orange</i> , <i>Red</i> , <i>Bold Red</i> , <i>Purple</i> , <i>White</i> , <i>Gray</i> .
<b>Show Creation Time</b>	Select to print the report date on the cover page.
<b>Show Data Range</b>	Select to print the data range on the cover page.
<b>Report Title</b>	Type a title in the <i>Report Title</i> field.
<b>Custom Text 1</b>	Enter custom text for the <i>Custom Text 1</i> field.
<b>Custom Text 2</b>	Enter custom text for the <i>Custom Text 2</i> field.



<b>Bottom Image</b>	Select <i>Choose</i> to open the <i>Choose a graphic</i> dialog box. Select an image, or select <i>Upload</i> to find an image on the management computer, then select <i>OK</i> to add the image at the bottom of the cover page.
<b>Footer Left Text</b>	Edit the text printed in the left hand footer of the cover page.
<b>Footer Right Text</b>	Edit the text printed in the left hand footer of the cover page. {default} prints the report creation date and time.
<b>Footer Background Color</b>	Select the cover page footer background color from the drop-down list. Select one of the following: <i>Bold Blue, Blue, Turquoise, Green, Bold Green, Yellow, Orange, Red, Bold Red, Purple, White, Gray, Transparent</i> .
<b>Reset to Default</b>	Select to reset the cover page settings to their default settings.

6. Click *OK* to save the configurations and return to the Settings tab.

## Managing reports

You can manage reports by going to *Reports > Report Definitions > All Reports*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a report to display the menu.

Option	Description
<b>Create New</b>	Creates a new report. You can choose whether to base the new report on a report template.
<b>Edit</b>	Edits the selected report.
<b>Delete</b>	Deletes the selected report.
<b>Clone</b>	Clones the selected report.
<b>Run report</b>	Generates a report.
<b>Folder</b>	Organize reports into folders.
<b>Import Report</b>	Imports a report from a management computer.
<b>Export Report</b>	Exports a report to a management computer.

## Organizing reports into folders

You can create folders to organize reports.

**To organize reports into folders:**

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Report Definitions > All Reports*.
3. Click *Folders* in the toolbar, and select *Create New Folder*.
4. Type a name in the dialog box that opens, and click *OK*. The folder is now displayed on the report list.
5. Drag and drop reports into the folder as desired.

## Importing and exporting reports

You can transport a report between FortiAnalyzer units. You can export a report from the FortiAnalyzer unit to the management computer. The report is saved as a .dat file on the management computer. You can then import the report file to another FortiAnalyzer unit.

**To export or import reports:**

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Report Definitions > All Reports*.
3. In the content pane, select a report, and select *Import* or *Export* from the *More* drop-down menu in the toolbar.

## Report template library



Because the cut, copy and paste functions need access to the clipboard of your operating system, some Internet browsers either block it when called from layout editor toolbar, or ask you to explicitly agree to that. Should accessing the clipboard by clicking the respective cut, copy and paste buttons from toolbar or context menu options be blocked, you can always perform these operations with keyboard shortcuts.

---

A report template defines the charts, and macros to use in the report as well as the layout of the content.

You can use the following items to create a report template:

- Text
- Images
- Tables
- Charts that reference datasets
- Macros that reference datasets

The datasets for charts and macros specify what data to use from indexed logs when you generate the report. You can also create custom charts and macros to use in report templates.

## Creating report templates

**To create a report template:**

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to the *Reports > Report Definitions > Templates*.

3. In the toolbar of the content pane, click *Create New*.
4. Set the following options:
  - a. Name
  - b. Description
  - c. Category
5. Use the toolbar to insert and format text and graphics for the template. In particular, use the FortiAnalyzer Chart and FortiAnalyzer Macro buttons to insert charts and macros into the template.  
For a description of the fields, see [Reports Layouts tab on page 115](#). For information about creating charts and macros, see [Creating charts on page 100](#) and [Creating macros on page 104](#).
6. Click *OK*.  
The new template is now displayed on the template list.

## Creating report templates by saving a report

You can save a report as a report template.

### To create a report template by saving a report:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Report Definitions > All Reports*.
3. In the content pane, select the report from the list, and click *Edit* in the tool bar.
4. On the *Layout* tab, click the *Save As Template* button in the toolbar.
5. In the *Save as Template* dialog box, set the following options, and click *OK*:
  - a. Name
  - b. Description
  - c. Category

The new template is now displayed on the template list.

## Viewing sample reports for predefined report templates

You can view sample reports for predefined report templates to help you visualize how the reports would look.

### To view sample reports:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to the *Reports > Report Definitions > Templates*.
3. In the content pane, click the *HTML* or *PDF* link in the *Preview* column of a template to view a sample report based on the template.

## Managing report templates

You can manage report templates in *Reports > Report Definitions > Templates*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a template to display the menu.

Option	Description
<b>Create New</b>	Create a new report template
<b>Edit</b>	Edit a report template. You can edit report templates that you created. You cannot edit predefined report templates.
<b>View</b>	Displays the settings for the predefined report template. You can copy elements from the report template to the clipboard, but you cannot edit a predefined report template.
<b>Delete</b>	Deletes the selected report template. You can delete report templates that you created. You cannot delete predefined report templates.
<b>Clone</b>	Clones the selected report template
<b>Rename</b>	Renames the selected report template. You can rename report templates that you created. You cannot rename predefined report templates.

## Chart library

### Creating charts



You can also create charts by using the Chart Builder that is available in *Log View*. See [Creating charts with Chart Builder on page 147](#).

#### To create charts:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Report Definitions > Chart Library*.
3. Click *Create New* in the toolbar.

Create Chart

Name:

Description:

Dataset:

Resolve Hostname:

Chart Type:

Data Bindings: ☒ Regular ☐ Ranked ☐ Drilldown

Columns

Click to add Column

Column 1

Title:

Width:  % (0 for Auto)

Data Binding:

Format:

Column 2

Title:

Width:  % (0 for Auto)

Data Binding:

Format:

☐ Order By

Show Top (0 for all results)

OK Cancel

4. Configure the settings for the new chart. The following table provides a description for each setting.

<b>Name</b>	Enter a name for the chart.
<b>Description</b>	Enter a description of the chart.
<b>Dataset</b>	Select a dataset from the drop-down list. See <a href="#">Datasets on page 105</a> for more information. The options will vary based on device type.
<b>Resolve Hostname</b>	Select to resolve the hostname. Select one of the following: <i>Inherit</i> , <i>Enabled</i> , or <i>Disabled</i> .
<b>Chart Type</b>	Select a graph type from the drop-down list; one of: <i>area</i> , <i>bar</i> , <i>donut</i> , <i>line</i> , <i>pie</i> , or <i>table</i> . This selection will affect the rest of the available selections.
<b>Data Bindings</b>	The data bindings vary depending on the chart type selected.
<b>area or line graphs</b>	
<b>X-Axis</b>	<p><i>Data Binding</i>: Select a value from the drop-down list. The available options will vary depending on the selected dataset.</p> <p><i>Label</i>: Enter a label for the axis.</p>
<b>Add line</b>	Select to add more lines.
<b>Lines</b>	<p>Enter the following options for each line:</p> <ul style="list-style-type: none"> <li>• <i>Data Binding</i>: Select a value from the drop-down list. The available options will vary depending on the selected dataset.</li> <li>• <i>Format</i>: Select a format from the drop-down list: <i>Bandwidth</i>, <i>Counter</i>, <i>Default</i>, or <i>Severity</i>.</li> <li>• <i>Type</i>: Select the type from the drop-down list: <i>Line Up</i> or <i>Line Down</i>.</li> <li>• <i>Legend</i>: Enter the legend text for the line.</li> </ul>
<b>bar</b>	
<b>X-Axis</b>	<p><i>Data Binding</i>: Select a value from the drop-down list. The available options will vary depending on the selected dataset.</p> <p><i>Only Show First</i>: Enter a numerical value. Only the first 'X' items will be displayed. Other items are bundled into the <i>Others</i> category.</p> <p><i>Overwrite label</i>: Enter a label for the axis.</p>
<b>Y-axis</b>	<p><i>Data Binding</i>: Select a value from the drop-down list. The available options will vary depending on the selected dataset.</p> <p><i>Overwrite label</i>: Enter a label for the axis.</p>
<b>Group By</b>	<p><i>Data Binding</i>: Select a value from the drop-down list. The available options will vary depending on the selected dataset.</p> <p><i>Show Top</i>: Enter a numerical value. Only the first 'X' items will be displayed. Other items can be bundled into the <i>Others</i> category.</p>
<b>Bundle rest into "Others"</b>	Select to bundle the rest of the results into an <i>Others</i> category.

<b>Order By</b>	Select to order by the X-Axis or Y-Axis.
<b>pie or donut graphs</b>	
<b>Category</b>	<p><i>Data Binding:</i> Select a value from the drop-down list. The available options will vary depending on the selected dataset.</p> <p><i>Label:</i> Enter a label for the axis.</p> <p><i>Show Top:</i> Enter a numerical value. Only the first 'X' items will be displayed. Other items can be bundled into the <i>Others</i> category.</p>
<b>Series</b>	<p><i>Data Binding:</i> Select a value from the drop-down list. The available options will vary depending on the selected dataset.</p> <p><i>Format:</i> Select a format from the drop-down list: <i>Bandwidth</i>, <i>Counter</i>, <i>Default</i>, <i>Percentage</i>, or <i>Severity</i></p> <p><i>Label:</i> Enter a label for the axis.</p>
<b>Bundle rest into "Others"</b>	Select to bundle the rest of the results into an <i>Others</i> category.
<b>table</b>	
<b>Table Type</b>	Select <i>Regular</i> , <i>Ranked</i> , or <i>Drilldown</i> .
<b>Add Column</b>	Select to add a column. Up to 15 columns can be added for a <i>Regular</i> table, <i>Ranked</i> tables have two columns, and <i>Drilldown</i> tables have three columns.
<b>Columns</b>	<p>The following column settings must be set:</p> <ul style="list-style-type: none"> <li>• <i>Column Title:</i> Enter a title for the column.</li> <li>• <i>Width:</i> Enter the column width as a percentage.</li> <li>• <i>Add Data Binding:</i> Add data bindings to the column. Every column must have at least one data binding. The maximum number varies depending on the table type.</li> <li>• <i>Data Binding:</i> Select a value from the drop-down list. The options vary depending on the selected dataset.</li> <li>• <i>Format:</i> Select a value from the drop-down list.</li> </ul>
<b>Order By</b>	Select what to order the table by. The available options will vary depending on the selected dataset.
<b>Bundle rest into "Others"</b>	Select to bundle the rest of the results into an <i>Others</i> category. This option is not available for regular tables.
<b>Show Top</b>	Enter a numerical value. Only the first 'X' items will be displayed. Other items can be bundled into the <i>Others</i> category for <i>Ranked</i> and <i>Drilldown</i> tables.
<b>Drilldown Top</b>	Enter a numerical value. Only the first 'X' items will be displayed. This options is only available for Drilldown tables.

5. Click OK.

## Managing charts

You can manage charts in *Reports > Report Definitions > Charts Library*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a chart to display the menu.

Option	Description
<b>Create New</b>	Create a new chart
<b>Edit</b>	Edit a chart. You can edit charts that you created. You cannot edit predefined charts.
<b>View</b>	Displays the settings for the selected predefined chart. You cannot edit a predefined chart.
<b>Delete</b>	Deletes the selected chart. You can delete charts that you create. You cannot delete predefined charts.
<b>Clone</b>	Clones the selected chart
<b>Import</b>	Import an exported FortiAnalyzer chart.
<b>Export</b>	Export one or more FortiAnalyzer charts.
<b>Show Predefined</b>	Displays the predefined charts
<b>Show Custom</b>	Displays the custom charts
<b>Search</b>	Lets you search for a chart by typing the chart name and pressing enter

## Viewing datasets associated with charts

To view datasets associated with charts:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Report Definitions > Charts*.
3. Select a chart, and click *View* in the tool bar.
4. In the *View Chart* pane, find the name of the dataset associated with the chart in the *Dataset* field.
5. Go to *Reports > Report Definitions > Datasets*.
6. In the *Search* box, type the name of the dataset.
7. Select the dataset that is found, and click *View* in the toolbar to view it.

## Macro library

### Creating macros

The FortiAnalyzer unit provides a selection of predefined macros. You can also create new macros, or clone and edit existing macros.

Macros are predefined to use specific datasets and queries. They are organized into categories, and can be added to, removed from, and organized in reports.



Macros are currently supported in FortiGate and FortiCarrier ADOMs only.

#### To create a new macro:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Report Definitions > Macro Library*, and click *Create New*. The *Create Macro* pane is displayed.

Create Macro

Name

Description

Dataset

App-Risk-App-Usage-By-Category

Query

select appcat, sum(coalesce(sentbyte, 0)+coalesce(rcvdbyte, 0)) as bandwidth from \$log where \$filter and logid\_to\_int(logid) not in (4, 7, 14) and nullifna(appcat) is not null group by appcat order by bandwidth desc

Data Binding

appcat

Display

Text

OK

Cancel

3. Provide the required information for the new macro.

<b>Name</b>	Enter a name for the macro.
<b>Description</b>	Enter a description of the macro.
<b>Dataset</b>	Select a dataset from the drop-down list. The options will vary based on device type.
<b>Query</b>	Displays the query statement for the dataset selected.
<b>Data Binding</b>	The data bindings vary depending on the dataset selected. Select a data binding from the drop-down list.
<b>Display</b>	Select a value from the drop-down list.

4. Click *OK*. The newly created macro is shown in the Macro library.



## Managing macros

You can manage macros by *Reports > Libraries > Macro Library*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a macro to display the menu.

Option	Description
<b>Create New</b>	Create a new macro
<b>Edit</b>	Edit the selected macro. You can edit macros that you created. You cannot edit predefined macros.
<b>View</b>	Displays the settings for the selected macro. You cannot edit a predefined macro.
<b>Delete</b>	Deletes the selected macro. You can delete macros that you create. You cannot delete predefined macros.
<b>Clone</b>	Clones the selected macro
<b>Show Predefined</b>	Displays the predefined macros
<b>Show Custom</b>	Displays the custom macros
<b>Search</b>	Lets you search for a macro by typing the chart name and pressing enter

## Viewing datasets associated with macros

To view datasets associated with macros:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Report Definitions > Macro Library*.
3. Select a macro, and click *View* (for predefined macros) or *Edit* (for custom macros) in the toolbar.
4. In the *View Macro* pane, find the name of the dataset associated with the macro in the *Dataset* field.
5. Go to *Reports > Report Definitions > Datasets*.
6. In the *Search* box, type the name of the dataset.
7. Double-click the dataset found to view it.

## Datasets

### Creating datasets

FortiAnalyzer datasets are collections of data from logs for monitored devices. Charts and macros reference datasets. When you generate a report, the datasets populate the charts and macros to provide data for the report.

Predefined datasets for each supported device type are provided, and new datasets can be created and configured.

#### To create a new dataset:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Report Definitions > Datasets*, and click *Create New*. The *Create Dataset* pane is displayed.
3. Provide the required information for the new dataset.

<b>Name</b>	Enter a name for the dataset.
<b>Log Type</b>	Select a log type from the drop-down list. <ul style="list-style-type: none"> <li>• The following log types are available for FortiGate: <i>Application Control, Intrusion Prevention, Content Log, Data Leak Prevention, Email Filter, Event, Traffic, Virus, VoIP, Web Filter, Vulnerability Scan, FCT Event, FCT Traffic, FCT Vulnerability Scan, Web Application Firewall</i>, and <i>GTP</i>.</li> <li>• The following log types are available for FortiMail: <i>Email Filter, Event, History</i>, and <i>Virus</i>.</li> <li>• The following log types are available for FortiWeb: <i>Intrusion Prevention, Event</i>, and <i>Traffic</i>.</li> </ul>
<b>Query</b>	Enter the SQL query used for the dataset.
<b>Add Variable</b>	Click the <i>Add</i> button to add variable, expression, and description information.
<b>Test query with specified devices and time period</b>	
<b>Time Period</b>	Use the drop-down list to select a time period. When selecting <i>Other</i> , enter the start date, time, end date, and time.
<b>Devices</b>	Select <i>All Devices</i> or <i>Specify</i> to select specific devices to run the SQL query against. Click the <i>Select Device</i> button to add multiple devices to the query.
<b>Test</b>	Select to test the SQL query before saving the dataset configuration.

4. Click *Test*.  
The query results are displayed. If the query is not successful, an error message appears in the results pane.
5. Click *OK*.

## Viewing the SQL query for an existing dataset

You can view the SQL query for a dataset, and test the query against specific devices or all devices.

#### To view the SQL query for an existing dataset:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Report Definitions > Datasets*.

3. Hover the mouse cursor over the dataset on the dataset list. The SQL query is displayed as a tooltip. You can also open the dataset to view the query in the *Query* field.,

## Managing datasets

You can manage datasets by going to *Reports > Report Definitions > Dataset*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a dataset to display the menu.

Option	Description
<b>Create New</b>	Create a new dataset.
<b>Edit</b>	Edit the selected dataset. You can edit datasets that you created. You cannot edit predefined datasets.
<b>View</b>	Displays the settings for the selected dataset. You cannot edit a predefined dataset.
<b>Delete</b>	Deletes the selected dataset. You can delete datasets that you create. You cannot delete predefined datasets.
<b>Clone</b>	Clones the selected dataset. You can edit cloned datasets.
<b>Validate</b>	Validate all datasets.
<b>Validate All Custom</b>	Validate all custom datasets.
<b>Search</b>	Lets you search for a dataset by typing the name of the dataset and pressing enter. To clear the search, delete the name from the search box.

## Output profiles

Output profiles allow you to define email addresses to which generated reports are sent and provide an option to upload the reports to FTP, SFTP, or SCP servers. Once created, an output profile can be specified for a report.

## Creating output profiles



You must configure a mail server before you can configure an output profile. See [Mail servers on page 185](#).

### To create output profiles:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Advanced > Output Profile*.
3. Click *Create New*. The *Create Output Profile* pane is displayed.

Create Output Profile

Name

Comments

Output Format ☒ PDF ☐ HTML ☐ XML ☐ CSV

☒ Email Generated Reports

Subject

Body

Recipients

Email Server	From	To
fortinet: smtp.fortinet.com	test@fortinet.com	test@fortinet.com

☒ Upload Report to Server

Server Type

Server

User

Password

Directory

☐ Delete file(s) after uploading

OK Cancel

4. Provide the following information, and click **OK**:

<b>Name</b>	Enter a name for the new output profile.
<b>Comments</b>	Enter a comment about the output profile (optional).
<b>Output Format</b>	Select the format or formats for the generated report. You can choose from PDF, HTML, XML, and CSV formats.
<b>Email Generated Reports</b>	Enable emailing of generated reports.
<b>Subject</b>	Enter a subject for the report email.
<b>Body</b>	Enter body text for the report email.
<b>Recipients</b>	Select the email server from the drop-down list and enter to and from email addresses. Select <i>Add New</i> to add another entry so that you can specify multiple recipients.
<b>Upload Report to Server</b>	Enable uploading of generated reports to a server.
<b>Server Type</b>	Select <i>FTP</i> , <i>SFTP</i> , or <i>SCP</i> from the drop-down list.
<b>Server</b>	Enter the server IP address.
<b>User</b>	Enter the username.
<b>Password</b>	Enter the password.
<b>Directory</b>	Specify the directory where the report will be saved.
<b>Delete file(s) after uploading</b>	Select to delete the generated report after it has been uploaded to the selected server.

## Managing output profiles

You can manage output profiles by going to *Reports > Advanced > Output Profile*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click an output profile to display the menu.

Option	Description
<b>Create New</b>	Create a new output profile.
<b>Edit</b>	Edit the selected output profile.
<b>Delete</b>	Delete the selected output profile.

## Report languages

You can specify the language of reports when creating a report. You can add new languages, and you can change the name and description of the languages. You cannot edit the predefined languages.

### Predefined report languages

FortiAnalyzer includes the following predefined report languages:

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

## Adding language placeholders

**To add a language placeholder:**

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Advanced > Language*.
3. Click *Create New* in the toolbar.
4. In the *New Language* pane, enter a name and description for the language, and click *OK*.  
A new language placeholder is created.



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

## Managing report languages

You can manage report languages by going to *Reports > Advanced > Language*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a language to display the menu.

Option	Description
<b>Create New</b>	Create a new report language placeholder.
<b>View</b>	View details about the selected report language.
<b>Edit</b>	Edit the selected report language. You cannot edit predefined report languages.
<b>Delete</b>	Delete the selected report language. You cannot delete predefined report languages.

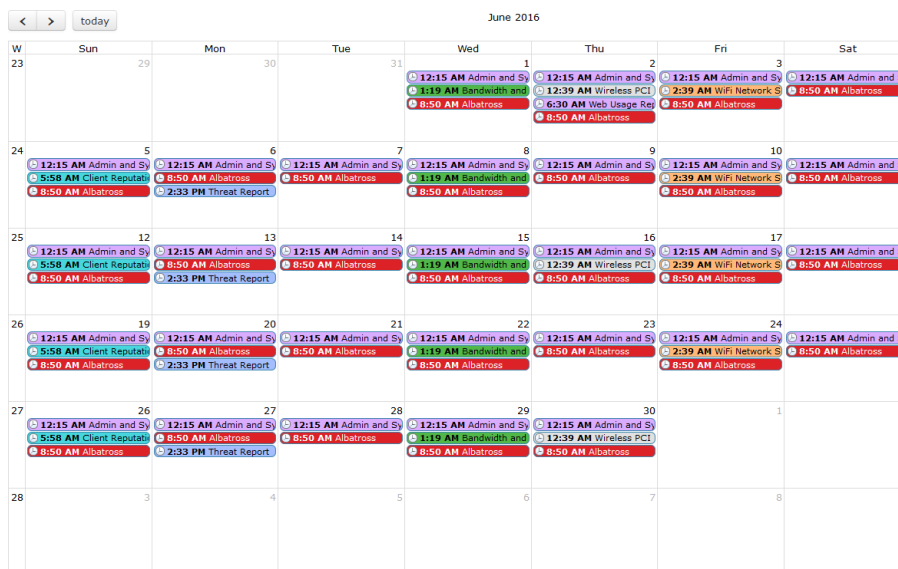
## Report calendar

You can use the report calendar to view all the reports that are scheduled for the selected month. You can edit or disable upcoming report schedules, as well as delete or download completed reports.

## Viewing all scheduled reports

To view all scheduled reports:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports > Advanced > Report Calendar*.



3. Hover the mouse cursor over a calendar entry to display the name, status, and device type of the scheduled report. You can double-click the calendar entry to go to the *Settings* tab of the report.
4. Click the left or right arrow at the top of the *Report Calendar* pane to change the month that is displayed. Click *Today* to return to the current month.

## Managing report schedules

You can manage report schedules in *Reports > Advanced > Report Calendar*.

### To edit a report schedule:

1. In *Report Calendar*, right-click an upcoming calendar entry, and select *Edit*.
2. In the *Settings* tab of the report that opens, edit the corresponding report schedule.

### To disable a report schedule:

- In *Report Calendar*, right-click an upcoming calendar entry, and select *Disable*.  
All scheduled instances of the report are removed from the report calendar. Completed reports remain in the report calendar.

### To delete or download a completed report:

- In *Report Calendar*, right-click a past calendar entry, and select *Delete* or *Download*. The corresponding completed report will be deleted or downloaded.

**Note:** You can only delete or download scheduled reports that have a status of *Finished*. You cannot delete scheduled reports with a status of *Pending*.

## Report references

### List of report templates

FortiAnalyzer includes report templates that you can use as it is or build upon when you create a new report. FortiAnalyzer provide different templates for different devices.

You can find report templates in the *Reports > Report Definitions > Templates* tree menu.

### FortiGate report templates

Template - 360-Degree Security Review	Template - PCI-DSS Compliance Review
Template - Admin and System Events Report	Template - Security Analysis
Template - Application Risk and Control	Template - Threat Report
Template - Bandwidth and Applications Report	Template - User Security Analysis

Template - Client Reputation	Template - VPN Report
Template - Data Loss Prevention Detailed Report	Template - Web Usage Report
Template - Detailed Application Usage and Risk	Template - WiFi Network Summary
Template - Email Report	Template - Wireless PCI Compliance
Template - IPS Report	Template - Top 20 Categories and Applications (Bandwidth)
Template - Top Allowed and Blocked with Timestamps	Template - Top 20 Categories and Applications (Session)
Template - Hourly Website Hits	Template - Top 20 Category and Websites (Session)
Template - Top 20 Category and Websites (Bandwidth)	Template - Top 500 Sessions by Bandwidth
Template - User Detailed Browsing Log	Template - User Top 500 Websites by Session
Template - User Top 500 Websites by Bandwidth	Template - FortiClient Default Report

### FortiCache report templates

Template - FortiCache Default Report

### FortiCarrier report templates

Template - FortiCarrier Default Report

### FortiClient report templates

Template - FortiClient Default Report

### FortiDDoS report templates

Template - FortiDDoS Default Report

### FortiMail report templates

Template - FortiMail Analysis Report

Template - FortiMail Default Report

### FortiSandbox report templates

Template - FortiSandbox Default Report



## FortiWeb report templates

Template - FortiWeb Default Report

## Reports Settings tab

The following options are available in the *Settings* tab:

Field	Description
<b>Time Period</b>	The time period that the report will cover. Select a time period, or select <i>Other</i> to manually specify the start and end date and time.
<b>Devices</b>	The devices that the report will include. Select either <i>All Devices</i> or <i>Specify</i> to add specific devices. Select the add icon to select devices.
<b>Type</b>	Select either <i>Single Report (Group Report)</i> or <i>Multiple Reports (Per-Device)</i> . This option is only available if multiple devices are selected.
<b>Enable Schedule</b>	Select to enable report template schedules.
<b>Enable Auto-Cache</b>	Select to assemble datasets before generating the report and as the data is available. This process uses system resources and is recommended only for reports that require days to assemble datasets. Disable this option for unused reports and for reports that require little time to assemble datasets.
<b>Generate PDF Report Every</b>	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.
<b>Start time</b>	Enter a starting date and time for the file generation.
<b>End time</b>	Enter an ending date and time for the file generation, or set it for never ending.
<b>Enable Notification</b>	Select to enable report notification.
<b>Output Profile</b>	Select the output profile from the drop-down list, or select <i>Create New</i> to create a new output profile. See <a href="#">Output profiles on page 107</a> .

## Filters section of Reports Settings tab

In the *Filters* section of the *Settings* tab, you can create and apply log message filters, and add an LDAP query to the report. The following options are available.

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

### Advanced Settings section of Reports Settings tab

The following options are available in the Advanced Settings section of the Settings tab.

Field	Description
<b>Language</b>	Select the report language. Select one of the following: <i>Default, English, French, Japanese, Korean, Portuguese, Simplified_Chinese, Spanish, or Traditional_Chinese</i> .
<b>Bundle rest into "Others"</b>	Select to bundle the uncategorized results into an <i>Others</i> category.
<b>Print Orientation</b>	Set the print orientation to portrait or landscape.
<b>Chart Heading Level</b>	Set the heading level for the chart heading.
<b>Hide # Column</b>	Select to hide the column numbers.
<b>Layout Header</b>	Enter header text and select the header image. The default image is <i>fortinet_logo.png</i> .
<b>Layout Footer</b>	Select either a default footer or custom footer. When selecting <i>Custom</i> , enter the footer text in the text field.
<b>Print Cover Page</b>	Select to print the report cover page. Select <i>Customize</i> to customize the cover page. See <a href="#">Customizing report cover pages on page 95</a> .
<b>Print Table of Contents</b>	Select to include a table of contents.
<b>Print Device List</b>	Select to print the device list. Select <i>Compact, Count, or Detailed</i> from the drop-down list.
<b>Print Report Filters</b>	Select to print the filters applied to the report.
<b>Obfuscate User</b>	Select to hide user information in the report.

Field	Description
<b>Resolve Hostname</b>	Select to resolve hostnames in the report. The default status is enabled.
<b>Allow Save Maximum</b>	Select a value between 1-1000 for the maximum number of reports to save.
<b>Color Code</b>	The color used to identify the report on the calendar. Select a color code from the drop-down list to apply to the report schedule. Color options include: <i>Bold Blue</i> , <i>Blue</i> , <i>Turquoise</i> , <i>Green</i> , <i>Bold Green</i> , <i>Yellow</i> , <i>Orange</i> , <i>Red</i> , <i>Bold Red</i> , <i>Purple</i> , and <i>Gray</i> .

## Reports Layouts tab



Because the cut, copy and paste functions need access to the clipboard of your operating system, some Internet browsers either block it when called from layout editor toolbar, or ask you to explicitly agree to that. Should accessing the clipboard by clicking the respective cut, copy and paste buttons from toolbar or context menu options be blocked, you can always perform these operations with keyboard shortcuts.

The following options are available in the layout tab (layout editor):

Field	Description
<b>Save as Template</b>	Select the save the layout as a template.
<b>Cut</b>	To cut a text fragment, start with selecting it. When the text is selected, you can cut it using one of the following methods: <ul style="list-style-type: none"> <li>• Select the cut button in the toolbar</li> <li>• Right-click and select cut in the menu</li> <li>• Use the <i>CTRL+X</i> shortcut on your keyboard.</li> </ul>
<b>Copy</b>	To cut a text fragment, start with selecting it. When the text is selected, you can cut it using one of the following methods: <ul style="list-style-type: none"> <li>• Select the cut button in the toolbar</li> <li>• Right-click and select cut in the menu</li> <li>• Use the <i>CTRL+C</i> shortcut on your keyboard.</li> </ul>
<b>Paste</b>	To paste a text fragment, start with cutting it or copying from another source. Depending on the security settings of your browser, you may either paste directly from the clipboard or use <i>Paste</i> dialog window.

Field	Description
<b>Paste as plain text</b>	If you want to paste an already formatted text, but without preserving the formatting, you can paste it as plain text. To achieve this, copy the formatted text and select the <i>Paste as plain text</i> button in the toolbar. If the browser blocks the editor toolbar's access to clipboard, a <i>Paste as Plain Text</i> dialog window will appear and you will be asked to paste the fragment into the text box using the <i>CTRL+V</i> keyboard shortcut.
<b>Paste from Word</b>	You can preserve basic formatting when you paste a text fragment from Microsoft Word. To achieve this, copy the text in a Word document and paste it using one of the following methods: <ul style="list-style-type: none"><li>• Select the Paste from Word button in the toolbar</li><li>• Use the <i>CTRL+V</i> shortcut on your keyboard.</li></ul>
<b>Undo</b>	Select to undo the last action. Alternatively, use the <i>CTRL+Z</i> keyboard shortcut to perform the undo operation.
<b>Redo</b>	Select to redo the last action. Alternatively, use the <i>CTRL+Y</i> keyboard shortcut to perform the redo operation.
<b>Find</b>	Select to find text in the report layout editor. Find consists of the following elements: <ul style="list-style-type: none"><li>• Find what: Is the text field where you enter the word or phrase that you want to find.</li><li>• Match case: Checking this option limits the search operation to words whose case matches the spelling (uppercase and lowercase letters) given in the search field. This means that the search becomes case-sensitive.</li><li>• Match whole word: Checking this option limits the search operation to whole words.</li><li>• Match cyclic: Checking this option means that after editor reaches the end of the document, the search continues from the beginning of the text. This option is checked by default.</li></ul>

Field	Description
<b>Replace</b>	<p>Select to replace text in the report layout editor. Replace consists of the following elements:</p> <ul style="list-style-type: none"> <li>• Find what: Is the text field where you enter the word or phrase that you want to find.</li> <li>• Replace with: Is the text field where you enter the word or phrase that will replace the search term in the document.</li> <li>• Match case: Checking this option limits the search operation to words whose case matches the spelling (uppercase and lowercase letters) given in the search field. This means that the search becomes case-sensitive.</li> <li>• Match whole word: Checking this option limits the search operation to whole words.</li> <li>• Match cyclic: Checking this option means that after editor reaches the end of the document, the search continues from the beginning of the text. This option is checked by default.</li> </ul>
<b>Image</b>	Select the <i>Image</i> button in the toolbar to insert an image into the report layout. Right-click an existing image to edit image properties.
<b>Table</b>	Select the <i>Table</i> button in the toolbar to insert a table into the report layout. Right-click an existing table to edit a cell, row, column, table properties or delete the table.
<b>Insert Horizontal Line</b>	Select to insert a horizontal line.
<b>Insert Page Break for Printing</b>	Select to insert a page break for printing.
<b>Link</b>	Select the <i>Link</i> button in the toolbar to open the <i>Link</i> dialog window. You can select to insert a URL, a link to an anchor in the text, or an email address. Alternatively, use the <b>CTRL+L</b> keyboard shortcut to open the <i>Link</i> dialog window.
<b>Anchor</b>	Select the <i>Anchor</i> button in the toolbar to insert an anchor in the report layout.
<b>FortiAnalyzer Chart</b>	Select to insert a FortiAnalyzer chart. Charts are associated with datasets that extract data from logs for the report.
<b>FortiAnalyzer Macro</b>	Select to insert a FortiAnalyzer macro. Macros are associated with datasets that extract data from logs for the report.
<b>Paragraph Format</b>	Select the paragraph format from the drop-down list. Select one of the following: Normal, Heading 1, Heading 2, Heading 3, Heading 4, Heading 5, Heading 6, Formatted, or Address.

Field	Description
<b>Font Name</b>	Select the font from the drop-down list. Select one of the following: Arial, Comic Sans MS, Courier New, Georgia, Lucida Sans Unicode, Tahoma, Times New Roman, Trebuchet MS, or Verdana.
<b>Font Size</b>	Select the font size from the drop-down list. Select a size ranging from 8 to 72.
<b>Bold</b>	Select the text fragment and then select the <i><b>Bold</b></i> button in the toolbar. Alternatively, use the <b>CTRL+B</b> keyboard shortcut to apply bold formatting to a text fragment.
<b>Italic</b>	Select the text fragment and then select the <i><b>Italic</b></i> button in the toolbar. Alternatively, use the <b>CTRL+I</b> keyboard shortcut to apply italics formatting to a text fragment.
<b>Underline</b>	Select the text fragment and then select the <i><b>Underline</b></i> button in the toolbar. Alternatively, use the <b>CTRL+U</b> keyboard shortcut to apply underline formatting to a text fragment.
<b>Strike Through</b>	Select the text fragment and then select the <i><b>Strike Through</b></i> button in the toolbar.
<b>Subscript</b>	Select the text fragment and then select the <i><b>Subscript</b></i> button in the toolbar.
<b>Superscript</b>	Select the text fragment and then select the <i><b>Superscript</b></i> button in the toolbar.
<b>Text Color</b>	<p>You can change the color of text in the report by using a color palette. To choose a color, select a text fragment and press the <i><b>Text Color</b></i> toolbar button. The <i><b>Text Color</b></i> drop-down menu that will open lets you select a color from a basic palette of 40 shades.</p> <p>If the color that you are after is not included in the basic palette, click the <i><b>More Colors</b></i> option in the drop-down menu. The <i><b>Select Color</b></i> dialog window that will open lets you choose a color from an extended palette.</p>
<b>Background Color</b>	You can also change the color of the text background.
<b>Insert/Remove Numbered List</b>	Select to insert or remove a numbered list.
<b>Insert/Remove Bulleted List</b>	Select to insert or remove a bulleted list.
<b>Decrease Indent</b>	To decrease the indentation of the element, select the <i><b>Decrease Indent</b></i> toolbar button. The indentation of a block-level element containing the cursor will decrease by one tabulator length.

Field	Description
<b>Increase Indent</b>	To increase the indentation of the element, select the <i>Increase Indent</i> toolbar button. The block-level element containing the cursor will be indented with one tabulator length.
<b>Block Quote</b>	Block quote is used for longer quotations that are distinguished from the main text by left and right indentation. It is recommended to use this type of formatting when the quoted text consists of several lines or at least 100 words.
<b>Align Left</b>	When you align your text left, the paragraph is aligned with the left margin and the text is ragged on the right side. This is usually the default text alignment setting for the languages with left to right direction.
<b>Center</b>	When you center your text, the paragraph is aligned symmetrically along the vertical axis and the text is ragged on the both sides. This setting is often used in titles or table cells.
<b>Align Right</b>	When you align your text right, the paragraph is aligned with the right margin and the text is ragged on the left side. This is usually the default text alignment setting for the languages with right to left direction.
<b>Justify</b>	When you justify your text, the paragraph is aligned with both left and right margin; the text is not ragged on any side. Instead of this, additional spacing is realized through flexible amount of space between letters and words that can stretch or contract according to the needs.
<b>Remove Format</b>	Select to remove formatting.

# Event Monitor

## About events

*Event Monitor* displays all of the events generated by event handlers. Event handlers define what messages to extract from the logs and display in *Event Monitor*. The system includes a number of predefined event handlers that you can enable to start populating *Event Monitor*. You can also create custom event handlers.



During the rebuild of the SQL database, you may not be able to see a complete list of historical events. However, you can always see events that are triggered from real-time logs. You can view the status of the SQL rebuild by checking the *Rebuilding DB* status in the *Notification Center*.

---

## How ADOMs affect events

When ADOMs are enabled, each ADOM has its own event handlers and lists of events. Make sure that you are in the correct ADOM before viewing *Event Monitor*. See also [Switching between ADOMs on page 28](#).

## Predefined event handlers

FortiAnalyzer includes a number of predefined event handlers that you can use to generate events for *Event Monitor*. You must enable predefined event handlers to start generating events.

## Logs used for events

*Event Monitor* displays events from indexed logs. Compressed logs are not used to generate events. For more information, see [Compressed logs and indexed logs on page 20](#).

## Event handlers

Event handlers define what messages to extract from logs and display in *Event Monitor*. You can enable predefined event handlers to generate events, or you can create and enable custom event handlers to generate events.

You can configure event handlers to generate events for a specific device, for all devices, or for the local FortiAnalyzer unit. You can create event handlers for FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiWeb, FortiSandbox devices, and syslog servers. In 5.2.0 or later, Event Management supports local FortiAnalyzer event logs.


You can also configure the system to send you alerts for event handlers. You can send the alert to an email address, SNMP community, or syslog server.



## Enabling event handlers

You must enable event handlers, including predefined event handlers, to generate events. If you want to configure alerts for predefined events handlers, you must edit the predefined event handler to configure alerts.

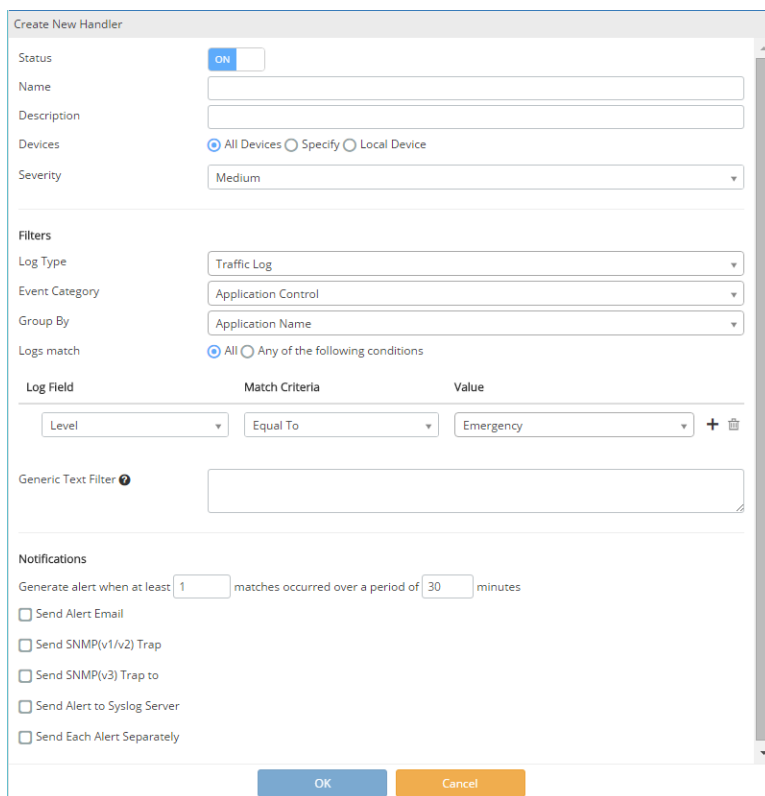
### To enable event handlers:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Event Monitor*.
3. Click *Event Handler List* in the toolbar.
4. Select an event handler on the list, and select *Enable* from the *More* drop-down menu in the toolbar.  
An "enabled" icon  is displayed right before the event handler's name.

## Creating custom event handlers

### To create a new event handler:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Event Monitor*.
3. Click *Event Handler List* in the toolbar.
4. Click *Create New* in the toolbar.
5. In the *Create New Handler* pane that is displayed, configure the settings.  
For a description of the fields, see [Create New Handler pane on page 128](#).



**Create New Handler**

Status: ☒ ON

Name:

Description:

Devices: ☒ All Devices ☐ Specify ☐ Local Device

Severity:

**Filters**

Log Type:

Event Category:

Group By:

Logs match: ☒ All ☐ Any of the following conditions

Log Field	Match Criteria	Value
<input type="text" value="Level"/>	<input type="text" value="Equal To"/>	<input type="text" value="Emergency"/>

Generic Text Filter:

**Notifications**

Generate alert when at least  matches occurred over a period of  minutes

☐ Send Alert Email

☐ Send SNMP(v1/v2) Trap

☐ Send SNMP(v3) Trap to

☐ Send Alert to Syslog Server

☐ Send Each Alert Separately

OK Cancel

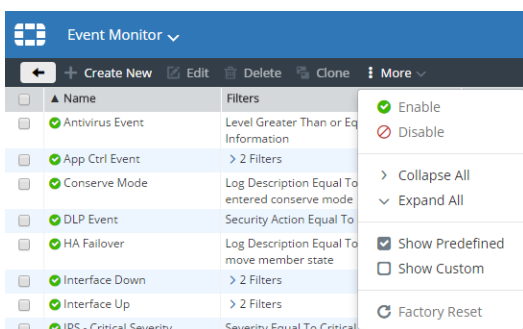
6. Click **OK**.

## Filtering event handlers by predefined and custom

You can filter the list of event handlers to by category: predefined and custom event handlers.

### To filter event handlers:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Event Monitor*.
3. From the *More* drop-down menu in the toolbar, use the *Show Predefined* and *Show Custom* check boxes to filter the event handlers.



## Searching event handlers

### To search event handlers:

1. Go to *Event Monitor*.
2. Type a search term in the search box in the top-right corner of the *Recent Events* pane.

## Resetting predefined event handlers to factory defaults

You can edit predefined event handlers to customize them for your needs. If you want to return the default event handlers to the factory settings, you can. The Factory Rest button is available only after you change one or more factory settings.

### To reset predefined event handlers:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Event Management > Event Handler*.
3. Select the *Show Predefined* check box.
4. Select a predefined event handler, and click *Edit*.
5. Edit the options.
6. Click *Factory Reset* to return the settings to the factory defaults.
7. Click *Return* to return to the *Event Handler* page.

## Managing event handlers

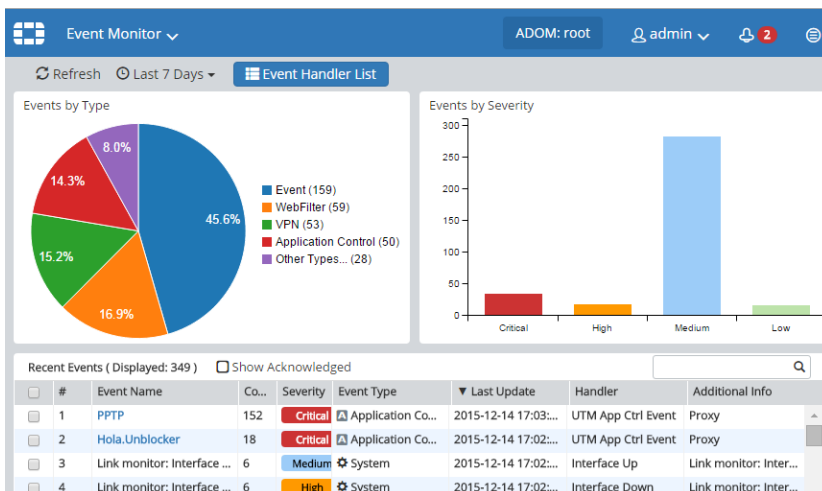
You can manage event handler by going to *Event Monitor > Event Handler List*. The following table shows the options available.

Option	Description
<b>Create New</b>	Create a new event handler. This option is available in the toolbar and right-click menu.
<b>Edit</b>	Edit the selected event handler.
<b>Delete</b>	Delete the selected event handler. You cannot delete predefined event handlers.
<b>Clone</b>	Clone the selected event handler. A cloned entry will have <i>Copy</i> added to its name field. You can rename the cloned entry while editing the event handler.
<b>Enable</b>	Enable the selected event handler to start generating events on the <i>Event Management &gt; All Events</i> page.
<b>Disable</b>	Disable the selected event handler to stop generating events on the <i>Event Management &gt; All Events</i> page.
<b>Factory Reset</b>	Return the settings for the selected predefined event handler to factory settings. This option is only available after you have edited a predefined event handler.

## Events

After event handlers start generating events, you can view the events and event details. *Event Monitor* provides a tabular view of recent events, as well as chart views of *Event by Type* and *Event by Severity*.

## Viewing event summaries



### To view event summaries:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Events Monitor*. You will see chart views of *Event by Type* and *Event by Severity* on the top of the page, followed by *Recent Events* in tabular view.
3. From the time drop-down list in the toolbar, select a time period to monitor, which will apply to all the views.
4. Check *Event by Type* and *Event by Severity* in chart views:
  - Hover the mouse over a graphical element to view more information.
  - Double-click the graphical element to view the corresponding filtered event list.

You can view event details by double-clicking an event summary entry. See [Viewing event details on page 124](#).

5. Check Recent Events in tabular view.
  - Sort entries on a column by clicking the column heading.
  - Include acknowledged events in the view by selecting the *Show Acknowledged* check box.
  - Search an event by any of the attributes in the Search box.
  - Click an Event Name hyperlink to view more information about the event.

You can view event details by double-clicking an event summary entry. See [Viewing event details on page 124](#).

## Viewing event details

### To view event details:

1. Drill-down to the event details page from event summaries in either tabular view or graphical view.
2. On the event details page, click an event instance to view the log details in the bottom pane.

- Click the **Back** button in the toolbar to return to event summary page.

#	Date/Time	Device ID	Action	Source IP	Destination IP	Virus	User
1	15:55:16	FGT37D4615800568	blocked	172.16.86.231	50.63.34.1	JS/Agent.NOI	
2	15:55:16	FGT37D4615800568	blocked	172.16.86.231	50.63.34.1	JS/Agent.NOI	
3	15:55:16	FGT37D4615800568	blocked	172.16.86.231	50.63.34.1	JS/Agent.NOI	
4	15:56:16	FGT37D4615800568	blocked	172.16.86.231	50.63.34.1	JS/Agent.NOI	
5	15:56:16	FGT37D4615800568	blocked	172.16.86.231	50.63.34.1	JS/Agent.NOI	
6	15:56:16	FGT37D4615800568	blocked	172.16.86.231	50.63.34.1	JS/Agent.NOI	
7	15:58:23	FGT37D4615800568	blocked	172.16.86.231	50.63.34.1	JS/Agent.NOI	
8	15:58:23	FGT37D4615800568	blocked	172.16.86.231	50.63.34.1	JS/Agent.NOI	
9	15:58:23	FGT37D4615800568	blocked	172.16.86.231	50.63.34.1	JS/Agent.NOI	

## Acknowledging events

When you acknowledge an event, it will be hidden from the event list.

### To acknowledge event(s):

- From the event list, select one or multiple events that you would like to acknowledge.
- Right-click and select **Acknowledge**. The acknowledged events are hidden from the event list.

If you want to view acknowledged events, select the **Show Acknowledged** check box.

## Event references

### List of predefined event handlers

FortiAnalyzer includes predefined event handlers for FortiGate and FortiCarrier devices that you can use to generate events.

Event Handler	Description
Antivirus Event	Severity: High Log Type: Traffic Log Event Category: Antivirus Group by: Virus Name Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Level Greater Than or Equal To Information</i></li> </ul>

Event Handler	Description
App CTRL Event	Severity: Medium Log Type: Traffic Log Event Category: Application Control Group by: Application Name Log messages that match any of the following conditions: <ul style="list-style-type: none"> <li><i>Application Category Equal To Botnet</i></li> <li><i>Application Category Equal To Proxy</i></li> </ul>
Conserve Mode	Severity: Critical Log Type: Event Log Event Category: System Group by: Message Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Log Description Equal To System services entered conserve mode</i></li> </ul>
DLP Event	Severity: Medium Log Type: Traffic Log Event Category: DLP Group by: DLP Rule Name Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Security Action Equal To Blocked</i></li> </ul>
HA Failover	Severity: Medium Log Type: Event Log Event Category: HA Group by: Log Description Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Log Description Equal To Virtual cluster move member</i></li> </ul>
Interface Down	Severity: High Log Type: Event Log Event Category: System Group by: Message Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Action Equal To interface-stat-change</i></li> <li><i>Status Equal To DOWN</i></li> </ul>
Interface Up	Severity: Medium Log Type: Event Log Event Category: System Group by: Message Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Action Equal To interface-stat-change</i></li> <li><i>Status Equal To UP</i></li> </ul>

Event Handler	Description
IPS - Critical Severity	Severity: Critical Log Type: IPS Group by: Attack Name Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Severity Equal To Critical</i></li> </ul>
IPS - High Severity	Severity: High Log Type: IPS Group by: Attack Name Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Severity Equal To High</i></li> </ul>
IPS - Medium Severity	Severity: Medium Log Type: IPS Group by: Attack Name Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Severity Equal To Medium</i></li> </ul>
IPS - Low Severity	Severity: Low Log Type: IPS Group by: Attack Name Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Severity Equal To Low</i></li> </ul>
IPsec Phase2 Down	Severity: Medium Log Type: Event Log Event Category: VPN Group By: VPN Tunnel Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Action Equal To phase2-down</i></li> </ul>
IPsec Phase2 Up	Severity: Medium Log Type: Event Log Event Category: VPN Group By: VPN Tunnel Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Action Equal To phase2-up</i></li> </ul>
Local Device Event	Devices: Local FortiAnalyzerSeverity: Medium Log Type: Event Log Event Category: Endpoint Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Level Greater Than or Equal To Warning</i></li> </ul>

Event Handler	Description
Power Supply Failure	Severity: Critical Log Type: Event Log Event Category: System Group by: Message Log messages that match any of the following conditions: <ul style="list-style-type: none"> <li><i>Action Equal To power-supply-monitor</i></li> <li><i>Status Equal To failure</i></li> </ul>
UTM Antivirus Event	Severity: High Log Type: Virus Group by: Virus Name Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Level Greater Than or Equal To Information</i></li> </ul>
UTM App CTRL Event	Severity: Medium Log Type: Application Control Group by: Application Name Log messages that match any of the following conditions: <ul style="list-style-type: none"> <li><i>Application Category Equal To Botnet</i></li> <li><i>Application Category Equal To Proxy</i></li> </ul>
UTM DLP Event	Severity: Medium Log Type: DLP Group by: DLP Rule Name Log messages that match all conditions: <ul style="list-style-type: none"> <li><i>Action Equal To Block</i></li> </ul>
UTM Web Filter Event	Severity: Medium Log Type: Web Filter Group by: Category Log messages that match any of the following conditions: <ul style="list-style-type: none"> <li><i>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</i></li> </ul>
Web Filter Event	Severity: Medium Log Type: Traffic Log Event Category: WebFilter Group by: Category Log messages that match any of the following conditions: <ul style="list-style-type: none"> <li><i>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</i></li> </ul>

## Create New Handler pane

Following is a description of the options available in the *Create New Handler* pane:



Field	Description
<b>Status</b>	Enable or disable the event handler.
<b>Name</b>	Edit the name if required.
<b>Description</b>	Enter a description for the event handler.
<b>Devices</b>	Select All Devices, select Specify and use the add icon to add devices. Select <i>Local FortiAnalyzer</i> if the event handler is for local FortiAnalyzer event logs. <i>Local FortiAnalyzer</i> is available in the root ADOM only and is used to query FortiAnalyzer event logs.
<b>Severity</b>	Select the severity from the drop-down list: <i>Critical, High, Medium, Low</i> .
<b>Log Type</b>	Select the log type from the drop-down list. The available options are: <i>Traffic Log, Event Log, Application Control, DLP, IPS, Virus, and Web Filter</i> . The <i>Log Type</i> is <i>Event Log</i> when <i>Devices</i> is <i>Local FortiAnalyzer</i> .
<b>Event Category</b>	Select the category of event that this handler will monitor from the drop-down list. The available options is dependent on the platform type. This option is only available when <i>Log Type</i> is set to <i>Traffic Log</i> and <i>Devices</i> is set to <i>All Devices</i> or <i>Specify</i> .
<b>Group By</b>	Select the criterion by which the information will be grouped. This option is not available when <i>Log Type</i> is set to <i>Traffic Log</i> .
<b>Log messages that match</b>	Select either All or Any of the Following Conditions. When <i>Devices</i> is <i>local FortiAnalyzer</i> , this option is not available.
<b>Add Filter</b>	Select the add icon to add log filters. When <i>Devices</i> is <i>local FortiAnalyzer</i> , this option is not available. You can only set one log field filter.
<b>Log Field</b>	Select a log field to filter from the drop-down list. The available options will vary depending on the selected log type.
<b>Match Criteria</b>	Select a match criteria from the drop-down list. The available options will vary depending on the selected log field.
<b>Value</b>	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.
<b>Delete</b>	Select the delete icon, to delete the filter. A minimum of one filter is required.
<b>Generic Text Filter</b>	Enter a generic text filter. For more information on creating a text filter, hover the cursor over the help icon.

Field	Description
<b>Generate alert when at least</b>	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.
<b>Send Alert Email</b>	Select the checkbox to enable. Enter an email address in the <i>To</i> and <i>From</i> text fields, enter a subject in the <i>Subject</i> field, and select the email server from the drop-down list. Select the add icon to add an email server. For information on creating a new mail server, see <a href="#">Mail servers on page 185</a> .
<b>Send SNMP(...) Trap to</b>	Select the checkboxes to enable these feature. Select an SNMP community or user from the requisite drop-down list. Select the add icon to add an SNMP community or user.
<b>Send Alert to Syslog Server</b>	Select the checkbox to enable this feature. Select a syslog server from the drop-down list. Select the add icon to add a syslog server. For information on creating a new syslog server, see <a href="#">Syslog servers on page 186</a>
<b>Send Each Alert Separately</b>	Select to send each alert individually, instead of in a groups.

# FortiView

## About FortiView

You can view summaries of log data in *FortiView* in both tabular and graphical formats. For example, you can view top threats to your network, top sources of network traffic, and top destinations of network traffic. For each summary view, you can drill down into details.

## How ADOMs affect the FortiView pane



When ADOMs are enabled, each ADOM has its own data analysis in *FortiView*.

## Logs used for FortiView

*FortiView* displays data from indexed logs. Data from compressed logs is not displayed in *FortiView*. For more information, see [Compressed logs and indexed logs on page 20](#).

## Description of FortiView

The following table describes the summary views available in *FortiView*.

	If you are running FortiOS 5.0.x, you must enable <i>Client Reputation</i> in the security profiles on the FortiGate in order to view entries in the <i>Top Threats</i> section of FortiView in FortiAnalyzer.	
	In FortiAnalyzer 5.4, the Endpoints view of <i>FortiView</i> is enabled for the default FortiClient ADOM, where you can view the lists of FortiClient endpoints that are registered to FortiClient EMS devices. Other views of <i>FortiView</i> will be added for the default FortiClient ADOM in future releases.	
Category	View	Description
Summary	An overview	An overview of most used <i>FortiView</i> summary views

Category	View	Description
<b>Threats</b>	Top Threats	Lists the top users involved in incidents, as well as information on the top threats to your network. The following incidents are considered threats: <ul style="list-style-type: none"> <li>• Risk applications detected by application control</li> <li>• </li> <li>• Intrusion incidents detected by IPS</li> <li>• Malicious web sites detected by web filtering</li> <li>• Malware/botnets detected by antivirus.</li> </ul>
	Threat Map	Displays a map of the world that shows the top traffic destination country by color. Threats are displayed when the level is equal to or greater than warning, and the source IP is a public IP address. See also <a href="#">Viewing the threat map on page 138</a> .
<b>Traffic</b>	Top Sources	Displays information about the sources of network traffic by displaying the source IP address, interface, and device
	Top Destinations	Displays information about the top destinations of network traffic by displaying the destination IP addresses and the application used to access the destination
	Top Countries	Displays a map of the world that shows
	Policy Hits	Lists the FortiGate policy hits by displaying the name of the policy, the name of the FortiGate device, and the number of hits
<b>Application &amp; Websites</b>	Top Applications	Displays information about the top applications being used on the network, including the application name, category, and risk level
	Top Cloud Applications	Displays information about the top cloud applications being used on the network
	Top Websites	Displays the top allowed and blocked web sites on the network
	Top Browsing Users	Displays the top web-browsing users. Includes the user name, number of sites visited, browsing time, and number of bytes sent and received.
<b>VPN</b>	SSL & Dialup IPsec	Displays the users who are accessing the network by using the following types of security over a virtual private network (VPN) tunnel: secure socket layers (SSL) and Internet protocol security (IPSEC)
	Site-to-Site IPsec	Displays the names of VPN tunnels with Internet protocol security (IPSEC) that are accessing the network

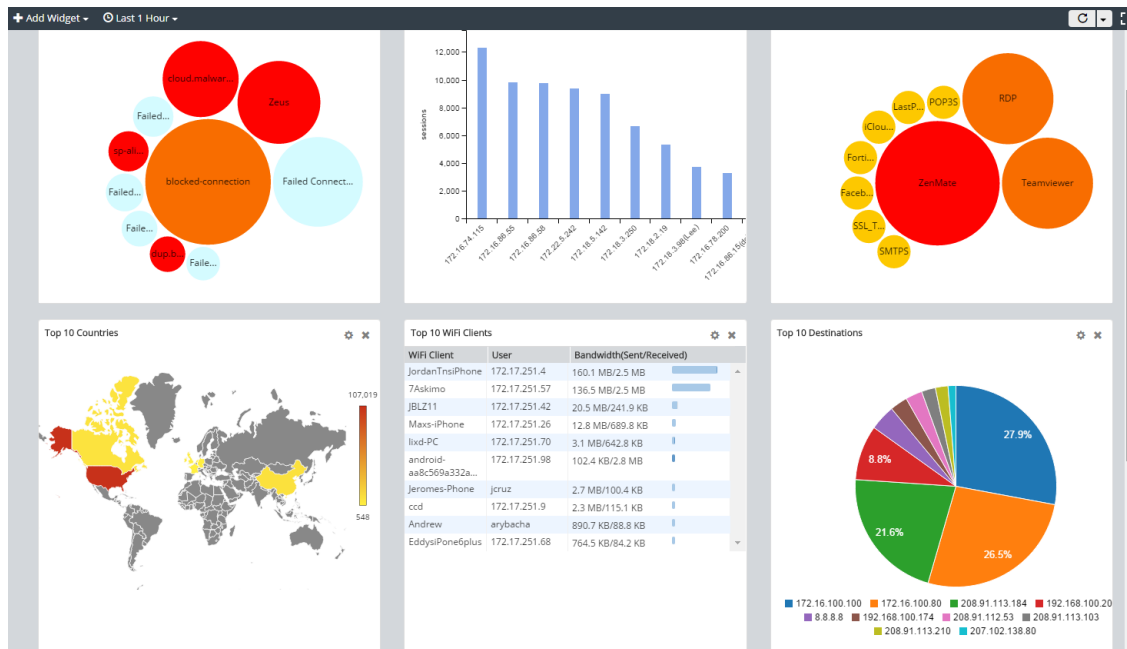
Category	View	Description
<b>WiFi</b>	Rogue APs	Displays the service set identifiers (SSID) of unauthorized WiFi access points on the network
	Authorized APs	Displays the names of authorized WiFi access points on the network
	Authorized SSIDs	Displays the service set identifiers (SSID) of authorized WiFi access points on the network
	WiFi Clients	Lists the names and IP addresses of the devices logged into the WiFi network
<b>System</b>	Admin Logins	Displays the users who logged into the managed device
	System Events	Displays events on the managed device
	Resource Usage	Displays device CPU, memory, logging, and other performance information for the managed device
	Storage Statistics	Displays statistics about the data policy and disk utilization for compressed logs and indexed logs
	Failed Authentication Attempts	Displays the IP addresses of the users who failed to log into the managed device
<b>Endpoints</b>	All Endpoints	Lists the FortiClient endpoints that are registered to FortiGate devices or FortiClient EMS devices.

## Using FortiView

When ADOMs are enabled, *FortiView* displays information for each ADOM. As a result, you should ensure that you are in the correct ADOM before viewing contents of *FortiView*. See also [Switching between ADOMs on page 28](#).

### Viewing FortiView summary page

When you go to *FortiView*, the first page that you will see is the *Summary* page. On the *Summary* page, you can get an overview of the most used summary views (a summary view is called a *widget* on the *Summary* page). You can view the details of each summary view in the same way as you do with a summary view on its own individual page (that you access through the tree menu). You can configure the overall view settings for the *Summary* page, as well as configure the view settings for each individual summary view/widget.

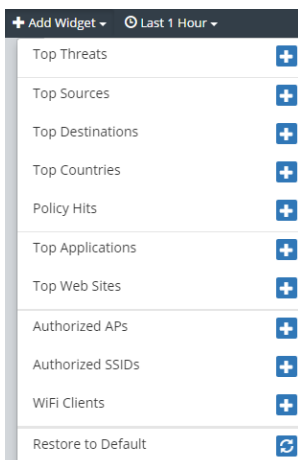


You can create multiple views/widgets for a FortiView summary. For example, you can create two Top Threats views: one of Top 10 Threats view in bubble chart format, and one of Top 20 Threats in table format.

## Configuring the overall view settings for the Summary page

### To add a widget to the Summary page:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *FortiView > Summary*.
3. In the content pane, click *Add Widget* in the tool bar, and select a FortiView summary from the list.



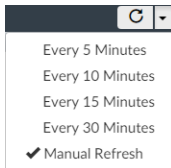
You can now see the newly added widget on the *Summary* page.

**To remove a widget from the Summary page:**

- Click the *Remove This Widget* button on the top-right corner of the widget.

**To specify a time period for all the views on the Summary page:**

- On the *FortiView Summary* page, select a time period from the *time* list **Last 1 Hour** in the toolbar.

**To refresh the view and/or set refresh rate:**

- On the *FortiView Summary* page, click the *Refresh Now* button in the toolbar or select a refresh rate from the drop-down menu.

**To switch to full-screen mode:**

- On the *FortiView Summary* page, click the *Full Screen* button in the toolbar.

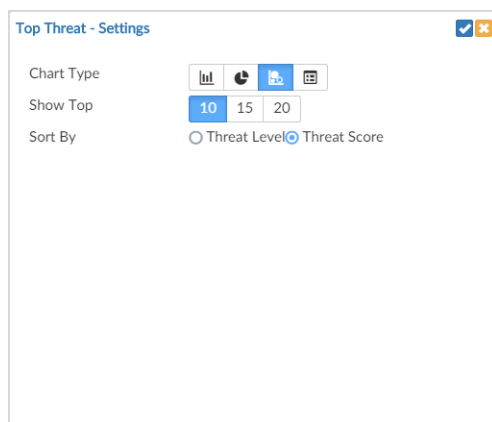
You can click the *Esc* key to exit full-screen mode.

**Viewing each widget on the Summary page**

You can view and drill down each summary view on the *Summary* page in the same way as you do with a summary view on its own individual page that you access through the tree menu. See [Viewing FortiView summaries in graphical format on page 136](#).

**Configuring the view settings for an individual widget:****To Configure the view settings for an individual widget:**

- On the *FortiView Summary* page, click the *Edit Settings* button on the top-right corner of the widget. The summary view flips to the settings panel.



- On the settings panel, configure the settings for the widget, such as *Chart Type*, *Show Top*, and *Sort By*.
- Click *OK* on the top-right corner to save the changes.

## Viewing FortiView summaries in tabular format

Tabular format is the default setting for viewing summary information. You can also view the information in graphical format.

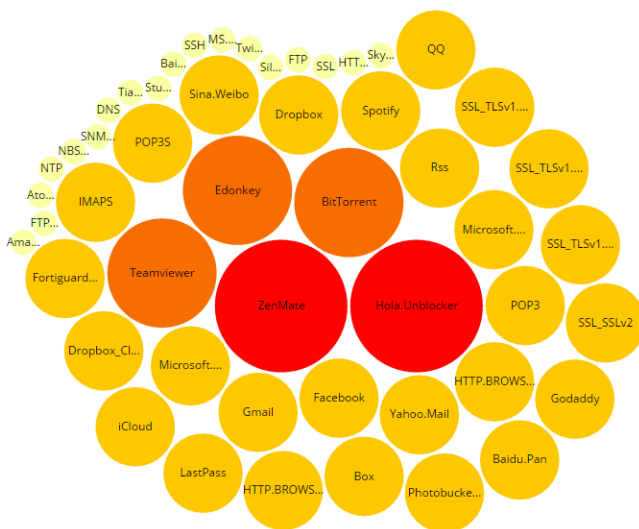
### To view summary information in tabular format:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *FortiView*, and select a summary view, such as *Top Applications*.
3. For the selected summary view, choose the tabular format by selecting the *Table* icon from the drop-down list in the top-right corner.
4. Sort entries by a column by clicking the column heading.
5. Double-click an entry to drill down. You can then view details about different dimensions of the entry in different tabs. Alternatively, you can right-click the entry and select a dimension to drill down.
6. You can continue drilling down by double-clicking an entry.
7. Click the *Back* button in the toolbar to return to the previous view.

## Viewing FortiView summaries in graphical format

### To view summary information in graphical format:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *FortiView*, and select a summary view from the tree menu, such as *Top Applications*.
3. For the selected summary view, select the *Bubble* icon from the drop-down list in the top-right corner.





4. Choose a sort method for the graphic from the *Sort By* list in the top-right corner.
5. Hover the mouse over a graphical element to view more information.
6. Click an element to drill down. You can then view details about different dimensions of the entry in different tabs.
7. You can continue drilling down by double-clicking an entry.
8. Click the *Back* button in the toolbar to return to the previous view.



## Filtering FortiView summaries

You can filter FortiView summaries in both the tabular and graphical view formats. You can filter information by using the *Add Filter* box in the toolbar or by right-clicking an entry and selecting a context-sensitive filter.

### To filter FortiView summaries by using the toolbar:

1. Specify filters in the *Add Filter* box.
  - Use Regular Search. In the selected summary view, click in the *Add Filter* box, select a filter from the drop-down list, and type a value. You can click NOT to negate the filter value. You can add multiple filters at a time, and connect them with "and" or "or".
  - Use Advanced Search. Click the *Switch to Advanced Search* icon  at the end of the *Add Filter* box. In the Advanced Search mode, you provide the whole search criteria (log field names and values) by typing. Click *Switch to Regular Search* icon  to go back to regular search.
2. In the *Device* list, select a device.
3. In the *Time* list, select a time period.
4. Click *Go*.

### To filter FortiView summaries by using the right-click menu:

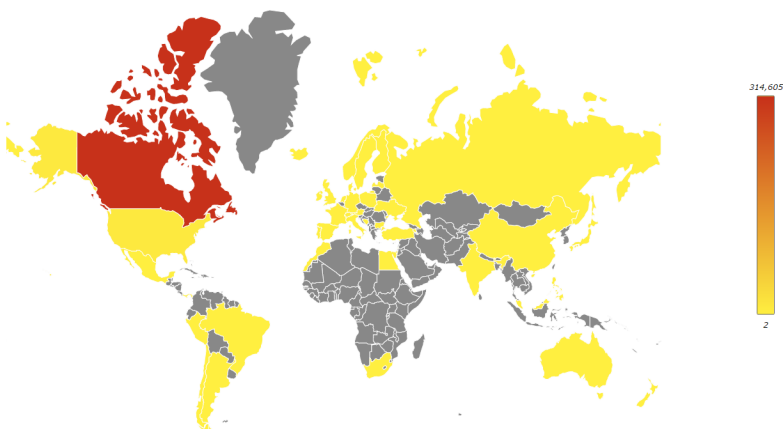
- In the selected summary view, right-click an entry, and select the filter criteria (*Search filter value*). Depending on the column in which your mouse is placed when you right-click, FortiView will use the column value of the selected entry as the filter criteria. This context-sensitive filter is only available for certain columns.

## Viewing a map of top countries

You can view a map of the *Traffic > Top Countries* summary view. The map shows the destination country.

### To view a map of top countries:

1. Go to *FortiView > Traffic > Top Countries*.
2. Select the *Map* icon from the drop-down list in the top-right corner.



3. Choose a sort method from the *Sort By* list in the top-right corner.
4. Hover the mouse over the map to view more information.

## Viewing the threat map

You can view an animated world map that displays threats from unified threat management logs. Threats are displayed in real time. No replay or additional details are available.



You must specify the longitude and latitude of the device to enable threats for the device to display in the threat map. You can edit the device settings to identify the geographical location of the device in *Device Manager*.

### To view the threat map:

1. Go to *FortiView > Threats > Threat Map*.
2. In the map, view the geographic location of the threats.
3. In the *Threat Window*, view the threat, level, and location.

## Viewing related logs

You can view the related logs for a FortiView summary in *Log View*. When you view the related logs, the same filters that you have applied to the FortiView summary are applied to the log messages.

### To view related logs for a FortiView summary:

- Right-click the entry and select *View Related Logs*.

## Exporting summary views to PDF

You can export to PDF both summary views and detail views, in both the tabular and graphical formats.

### To export information to PDF:

- In a selected summary or detail view, click the *Download as PDF* button in the top-right corner.

## Monitoring disk usage for devices

You can monitor how much FortiAnalyzer disk space the logs use. If you are using ADOMs, the disk usage is displayed per ADOM. If you are not using ADOMs, the disk usage is displayed for all log files generated by all devices managed by the FortiAnalyzer unit.

### To monitor disk usage for devices:

1. Go to *FortiView > System > Resource Usage*.
2. Click the *Return* button to return to the previous view.

## Viewing log storage statistics

You can monitor the data policy and disk utilization statistics for compressed logs and indexed logs. See also [Compressed logs and indexed logs on page 20](#).

**To view log storage statistics:**

1. Go to *FortiView > System > Storage Statistics*.
2. Hover the mouse over the charts to display tooltips.
3. For the Analytic Details and Archive Details line charts, you can click on a data point to drill down into more details, with a breakdown by device.

The following table describes the various charts:

Charts	Description
<b>Analytic Policy</b>	Displays information about the data policy for indexed logs. You can see the number from the <i>Keep Indexed Logs for Analytics</i> setting for the data policy, for example 14 days. Under <i>Quota Usage</i> , you can also see how much of the total allotted storage space is free and used.
<b>Analytic Details</b>	Provides a chart that shows how much disk space is consumed each day by indexed logs. The blue line shows actual usage, and a red line shows the maximum allotted disk space. Hover the mouse over the chart for more details. Click the chart to drill down into more details with a breakdown by device. Keep in mind that logs are automatically purged from the database earlier than the data policy specifies when the FortiAnalyzer unit starts to run out of space.
<b>Archive Policy</b>	Displays information about the data policy for compressed logs. You can see the number from the <i>Keep Compressed Logs for Retention</i> setting for the data policy, for example 180 days. Under <i>Quota Used</i> , you can also see how much of the total allotted storage space is free and used.
<b>Archive Details</b>	Provides a chart that shows how much disk space is consumed each day for compressed logs. The blue line shows actual usage, and a red line shows the maximum allotted disk space. Hover the mouse over the chart for more details. Click the chart to drill down into more details with a breakdown by device. Keep in mind that compressed logs are automatically deleted from the FortiAnalyzer unit earlier than the data policy specifies if the FortiAnalyzer unit starts to run out of space.

## Examples of using FortiView

Following are several examples of how you can use FortiView to find information about your network.

### Finding application and user information

Company ABC has over 1000 employees using a variety of applications across different divisional areas, including supply chain, accounting, facilities and construction, administration, and IT.

The administration team received a \$6000 invoice from a software provider to license an application called Widget-Pro. According to the software provider, an employee at Company ABC is using Widget Pro software.

The system administrator wants to find who is using applications that are not in the company's list of approved applications. The administrator also wants to determine whether the user is unknown to FortiGuard signatures, identify the list of users, and perform an analysis of their systems.

**To find the application and user info:**

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *FortiView > Applications & Websites > Top Applications*.
3. Click the *Add Filter* box, select *Application*, type *Widget-Pro*, and click *Go*.
4. If you do not find the application in the filtered results, go to *Log View > Traffic*.
5. Click the *Add Filter* box, select *Source*, type the source IP address, and click *Go*.

## Finding unsecured wireless access points

AAA Electronics has multiple access points in their stores for their wireless point-of-sale and mobile devices used by the sales team.

War-driving hackers found an unsecured wireless connection in the network at AAA Electronics. Hackers were able to connect to the network and install a program for stealing personal data.

The network administrator monitors unknown applications by using FortiAnalyzer alerts and was informed that an unauthorized program had been installed. Following an investigation, the administrator determined that the program secured a wireless access point. The administrator now wants to determine if any of the other AAA Electronics stores has insecure access points.

**To find information on unsecured wireless access points:**

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *FortiView > WiFi > Rogue APs* to view the list of unsecured wireless or rogue access points.

## Analyzing and reporting on network traffic

A new administrator starts at #1 Technical College. The school has a free WiFi for students on the condition that they accept the terms and policies for school use.

The new administrator is asked to do an analysis and report on the top source and destinations visited by students as well as the source and destinations that consume the most bandwidth and the number of attempts to visit blocked sites.

**To review the source and destination traffic and bandwidth:**

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *FortiView > Traffic > Top Sources*.
3. Go to *FortiView > Traffic > Top Destinations*.

# Log View

## About Log View

You can view the traffic log, event log, or security log information per device or per log array.



When rebuilding the SQL database, Log View will not be available until after the rebuild is completed. Select the *Show Progress* link in the message to view the status of the SQL rebuild.

## How ADOMs affect the Log View tab

When ADOMs are enabled, each ADOM has its own information displayed in *Log View*.

## Logs used for Log View

*Log View* displays log messages from indexed logs and compressed logs:

- Historical logs and Real-time logs in *Log View* are from indexed logs.
- *Log Browse* can display logs from both the current, active log file and any of the compressed log files.

For more information, see [Compressed logs and indexed logs on page 20](#).

## Log arrays in FortiAnalyzer 5.2.0 and later

The concept of log array changed between FortiAnalyzer 5.0.6 and FortiAnalyzer 5.2.0.

In FortiAnalyzer 5.0.6 and earlier, log arrays can be treated as a single device which has its own SQL database. The size of its database is enforced by the log array quota.

In FortiAnalyzer 5.2.0 and later, log array is only a grouping concept which is used to display logs or generate reports for a group of devices. It has no SQL database and does not occupy additional disk space.

## Types of logs collected for each device

Your FortiAnalyzer device can collect logs from managed FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiSandbox, FortiWeb, FortiClient, and syslog servers. Following is a description of the types of logs that FortiAnalyzer collects from each type of device:

Device Type	Log Type
FortiAnalyzer	Event

Device Type	Log Type
<b>FortiGate</b>	Traffic Event: Compliance Events, Endpoint, HA, System, Router, VPN, User, WAN Opt. & Cache, and Wireless Security: Vulnerability Scan, Antivirus, Web Filter, Application Control, Intrusion Prevention, Email Filter, Data Leak Prevention, Web Application Firewall FortiClient VoIP Content logs are also collected for FortiOS 4.3 devices.
<b>FortiCarrier</b>	Traffic, Event, GTP
<b>FortiCache</b>	Traffic, Event, Antivirus, Web Filter
<b>FortiClient</b>	Traffic, Event, Vulnerability Scan
<b>FortiDDoS</b>	Event, Intrusion Prevention
<b>FortiMail</b>	History, Event, Antivirus, Email Filter
<b>FortiManager</b>	Event
<b>FortiSandbox</b>	Malware, Network Alerts
<b>FortiWeb</b>	Event, Intrusion Prevention, Traffic
<b>Syslog</b>	Generic

## Traffic 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.

## Event logs

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

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



The logs displayed on your FortiAnalyzer are dependent on the device type logging to it and the features enabled. FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiWeb, FortiSandbox, FortiClient and Syslog logging is supported. ADOMs must be enabled to support non-FortiGate logging.

For more information on logging see the *Logging and Reporting for FortiOS Handbook* in the [Fortinet Document Library](#).



When rebuilding the SQL database, Log View will not be available until after the rebuild is completed. Although you can view older logs, new logs will not be inserted into the database until after the rebuild is completed. Select the *Show Progress* link in the message to view the status of the SQL rebuild.

## Log messages

You can view the traffic log, event log, or security log information per device or per log array.

### Viewing the log message list of a specific log type

When ADOMs are enabled, *Log View* displays information for each ADOM. As a result, you should ensure that you are in the correct ADOM before viewing contents of *Log View*. See also [Switching between ADOMs on page 28](#).

You can find FortiMail and FortiWeb logs in their respective default ADOMs.

#### To view the log message list:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Log View*, and select a type (or subtype) of logs from the following: *Traffic*, *Event*, or *Security*.  
The corresponding log messages list is displayed.

### Viewing log message details

#### To view log message details:

1. Select a log message from the log message list.
2. Click *Display Details* in the bottom right corner. The log message details are displayed in the bottom pane.

Add Filter											
All Devices Last 4 hours GO											
Column Settings Tools											
#	Date/Time	Threat	Action	Source	Destination IP	Service	Application	Destination Country	Policy ID	Policy UUID	
1	14:34:59			172.18.2.19	88.221.81.195	DNS	DNS				
2	14:34:59			172.16.68.94	213.199.179.169	udp/40014	Skype				
3	14:34:59			FortinetLeizhang (Lei)	192.168.100.174	RSH	RSH				
4	14:34:59			Sordonjin (GORDON-PC)	172.16.95.187	HTTPS	HTTPS				
5	14:34:59			172.16.69.132	8.8.8.8	DNS	DNS				
6	14:34:59	262144	DNS error	172.16.69.132	8.8.8.8	53/udp					
7	14:34:59			Kyu (KEVIN-OPTIPLEX-7020)	172.16.100.100	DNS	DNS				
8	14:34:59			172.16.79.207	65.55.223.29	udp/40021	Skype				
9	14:34:59			Sordonjin (GORDON-PC)	172.16.95.187	HTTPS	HTTPS				
10	14:34:59			FMG-LAB-PC	208.91.112.136	HTTPS	HTTPS				
11	14:34:59			Simon (Simon-deskstop)	172.16.100.80	DCE-RPC	DCE-RPC				
12	14:34:59			172.16.116.213	192.168.100.174	RSH	RSH				
13	14:34:59			172.16.79.207	65.55.223.29	udp/40021	Skype				
14	14:34:59			Rainxiaole (Rainxiaole-PC)	91.133.11.54	tcp/35470	tcp/35470				

## Customizing displayed columns

The columns displayed in the log message list can be customized and reordered as needed.

### To customize what columns to display:

1. In the log message list view, click *Column Settings* in the toolbar.
2. From the drop-down list that is displayed, select a column to hide or display.



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

3. To add more columns, select *More Columns*.

In the *Column Settings* dialog box that opens, you can show or hide columns by selecting and deselecting the columns.

4. To reset to the default columns, click *Reset to Default*.
5. Click *OK* to apply your changes.

### To change the order of the displayed columns:



- Place the cursor in the column header area, and then move a column by dragging and dropping.



## Filtering log messages

You can filter log summaries by using the *Add Filter* box in the toolbar or by right-clicking an entry and selecting a context-sensitive filter.

### To filter log summaries by using the toolbar:



1. Specify filters in the *Add Filter* box.
  - Use Regular Search. In the selected summary view, click in the *Add Filter* box, select a filter from the drop-down list, and type a value. You can click on an operator to use it, such as greater than (>), less than (<), OR, and NOT. You can add multiple filters at a time, and connect them with "and" or "or".
  - Use Advanced Search. Click the *Switch to Advanced Search* icon  at the end of the *Add Filter* box. In the Advanced Search mode, you provide the whole search criteria (log field names and values) by typing. Click *Switch to Regular Search* icon  to go back to regular search.



From the *Tools* drop-down menu in the tool bar, you can use the *Case Sensitive Search* check box to specify whether you want Log View to treat the filter value that you type case-sensitive or not.

2. In the *Device* list, select a device.
3. In the *Time* list, select a time period.
4. Click *Go*.

### To filter log summaries by using the right-click menu:

- In a log message list view, right-click an entry, and select a filter criteria. The search criteria with a  icon will return entries that match the filter values, while the search criteria with a  icon will return entries that negate the filter values.

Depending on the column in which your mouse is located when you right-click, *Log View* will use the column value of the selected entry as the filter criteria. This context-sensitive filter is only available for certain columns.

## Filtering FortiClient log messages in FortiGate traffic logs

For FortiClient endpoints that are registered to FortiGate devices, you can filter log messages in FortiGate traffic log files that are triggered by FortiClient.

### To Filter FortiClient log messages:

1. Go to *Log View > Traffic*.
2. In the *Add Filter* box, type `fct_devid=*`, and select *Go*. A list of FortiGate traffic logs that are triggered by FortiClient is displayed.
3. In the message log list, select a FortiGate traffic log to view the details in the bottom pane.
4. Click the *FortiClient* tab, and double-click a FortiClient traffic log to see details.  
The *FortiClient* tab is available only when the FortiGate traffic logs reference FortiClient traffic logs.

## Viewing search examples

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

```
* Basic search
Example: srcip=172.16.86.11 service=HTTP

* Search with 'or'
Example: srcip=172.16.* or srcip=172.18.*

* Search with 'not'
Example: -srcip=172.16.86.11 and -service=HTTP

* Wildcard is supported.
```

The first example will search for log messages with a source IP address of 172.16.86.11 and a service of HTTP. Because it is not specified, the `and` operator is assumed, meaning that both conditions must be met for the log message to be included in the search results.

The second example will search for any log messages with source IP addresses that start with either 172.16 or 172.18. Notice the use of the `*` wildcard. The use of the `or` operator means that either condition can be met for the log message to be included in the search results.

The third example will search for any log message that do not have a source IP address of 172.16.86.11 and a service of HTTP. The use of the `and` operator means that both conditions must be met for the log message to be excluded from the search results.

## Viewing historical and real-time logs

By default, historical logs are displayed. *Custom View* and *Chart Builder* are only available in historical log view.

### To view real-time logs:

- In the log message list view, select *Real-time Log* from the *Tools* drop-down menu in the toolbar.  
To switch back to historical log view, select *Historical Log* from the *Tools* drop-down menu.

## Viewing raw and formatted logs

By default, formatted logs are displayed. The selected log view will affect available view options. You cannot customize the columns when viewing raw logs.

### To view raw logs:

- In the log message list view, select *Display Raw* from the *Tools* drop-down menu in the toolbar.  
To switch back to formatted log view, select *Display Formatted* from the *Tools* drop-down menu in the toolbar.

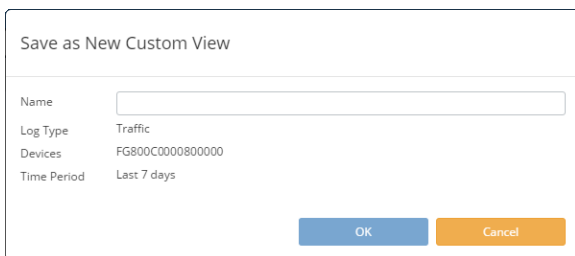
For more information about FortiGate raw logs, see the *FortiGate Log Message Reference* in the [Fortinet Document Library](#). For more information about raw logs of other devices, see the *Log Message Reference* for the platform type.

## Custom views

You can use *Custom View* to save a filter setting, device selection, and time period that you have specified so that you can go to this view at any time to view results without having to re-specify these criteria.

### To create a new custom view:

- Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
- Go to *Log View*, and select a log type.
- In the content pane, customize the log view as you want, for example, by adding filters, specifying devices, or specifying a time period.
- Select *Custom View* from *Tools* in the tool bar. The *Create New Custom View* dialog box opens.

A dialog box titled "Save as New Custom View". It contains four read-only fields: "Name" (with an empty text input), "Log Type" (Traffic), "Devices" (FG800C0000800000), and "Time Period" (Last 7 days). At the bottom right are "OK" and "Cancel" buttons.

Save as New Custom View	
Name	<input type="text"/>
Log Type	Traffic
Devices	FG800C0000800000
Time Period	Last 7 days
<div>OK Cancel</div>	

5. In the Name field, type a name for the new custom view. All other fields are read-only.
6. Click **OK**. The custom view is now displayed under *Log View > Custom View*.

#### To edit a custom view:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to the *Log View*, and select a log type.
3. On the tree menu, select the custom view that you want to edit under *Custom View*.
4. In the tool bar, edit the filter settings, and click **GO**.
5. In the tool bar, select *Custom View* from *Tools*.
6. In the *Create New Custom View* dialog box that opens, click **Save** to save the changes to the existing custom view, or click **Save as** to save the changes to a new custom view.
7. Click **OK**.

## Downloading log messages

Historical log messages can be downloaded to the management computer as a text or CSV file. Real-time log messages cannot be downloaded.

#### To download log messages:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Log View*, and select a log type.
3. In the tool bar, select *Download* from the *Tools* drop-down menu.
4. In the *Download Logs* dialog box that opens, configure the download options:
  - Select a log format from the *Log file format* drop-down list, either *Text* or *CSV*.
  - Select *Compress with gzip* to compress the downloaded file.
  - Select *Current Page* to download only the current log message page, or *All Pages* to download all the pages in the log message list.
5. Click **OK**.

## Creating charts with Chart Builder

*Log View* includes a Chart Builder that you can use to build custom charts for each type of log messages.

#### To create charts with Chart Builder:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Log View*, and select a log type.
3. Click *Chart Builder* in the toolbar.

4. In the *Chart Builder* dialog box that opens, complete the options to configure the chart. For a description of the fields, see "[Log View references](#)" on page 150. You can preview the chart in the *Preview* box.
5. Click **Save**.

For more information about creating charts, see [Chart library on page 100](#)

## Log arrays

*Log Array* has been relocated to *Log View* from *Device Manager*. Upon upgrading to FortiAnalyzer 5.2.0 and later, all previously configured log arrays will be imported. In FortiAnalyzer 5.0.6 and earlier, when creating a Log Array with both devices and VDOMs, you need to select each device and VDOM to add it to the Log Array. In FortiAnalyzer 5.2.0 and later, when selecting to add a device with VDOMs, all VDOMs are automatically added to the Log Array.

## Creating log arrays

**To create a new log array:**

1. Go to *Log View > Log Array*.
2. In the content pane, click *Create New* in the toolbar.
3. In the *Create New Log Array* dialog box that opens, configure the options.
4. Click **OK**. The newly created log array is shown in the log array list.

## Managing log arrays

You can manage log arrays in *Log View > Log Array*.

Option	Description
<b>Create New</b>	Create a new log array.
<b>Edit</b>	Edit the selected log array.
<b>Delete</b>	Delete the selected log array.

## Log Browse

When a log file reaches its maximum size or a 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 by using the CLI on page 85](#).)

You can view logs in the compressed phase of the log workflow in *Log Browse*. *Log Browse* displays log files stored for both devices and the FortiAnalyzer itself.

## Browsing log files

### To view log files:

1. Go to *Log View > Log Browse*
2. Select a log file, and click *Display* in the toolbar to open the log file and display the log messages in formatted view. You can perform all the same actions as with the log message list. See [Viewing log message details on page 143](#).

<span>Display</span> <span>Delete</span> <span>Download</span> <span>Import</span> <span>Search...</span>							
<input type="checkbox"/> ▲ Device	Serial Number	VDOM	Type	Log Files	From	To	Size(bytes)
<input type="checkbox"/> FG800C3912801080	FG800C3912801080	root	Event.	elog.log	Mon Oct 19 11:09:43 2015	Tue Nov 3 15:32:40 2015	3,013,855
<input type="checkbox"/> FG800C3912801080	FG800C3912801080	root	Traffic.	tllog.log	Tue Nov 3 15:29:29 2015	Tue Nov 3 15:33:26 2015	29,034,845
<input type="checkbox"/> FG800C3913802271	FG800C3913802271	root	Event.	elog.log	Thu Dec 10 16:14:29 2015	Mon Dec 14 15:08:36 2015	196,994,162
<input type="checkbox"/> FG800C3913802271	FG800C3913802271	root	Traffic.	tllog.log	Mon Dec 14 11:11:49 2015	Mon Dec 14 15:08:36 2015	137,316,667
<input type="checkbox"/> FGT37D4615800568	FGT37D4615800568	root	Event.	elog.log	Sun Dec 13 17:39:20 2015	Mon Dec 14 15:08:37 2015	121,906,049
<input type="checkbox"/> FGT37D4615800568	FGT37D4615800568	root	Traffic.	tllog.log	Mon Dec 14 15:06:51 2015	Mon Dec 14 15:08:37 2015	76,985,646
<input type="checkbox"/> FGT37D4615800568	FGT37D4615800568	root	Traffic.	tllog.1450134096.log.gz	Mon Dec 14 15:01:36 2015	Mon Dec 14 15:06:51 2015	35,530,685
<input type="checkbox"/> FGT37D4615800568	FGT37D4615800568	root	Traffic.	tllog.1450133752.log.gz	Mon Dec 14 14:55:52 2015	Mon Dec 14 15:01:36 2015	38,151,943
<input type="checkbox"/> FGT37D4615800568	FGT37D4615800568	root	Traffic.	tllog.1450133466.log.gz	Mon Dec 14 14:51:06 2015	Mon Dec 14 14:55:52 2015	38,496,563

## 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.

### To import a log file:

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Log View > Log Browse*.
3. Click *Import* in the toolbar. The *Import Log File* dialog box opens.
4. 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.
5. In the *File* field, click *Choose Files* and specify the log file on the management computer.
6. Click *OK*. A message appears, stating that the upload is beginning, but will be canceled if you leave the page.
7. Click *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.



If you have the *Delete log files after uploading* option enabled (under *System Settings > Device Log Settings > Registered Device Logs > Upload logs using a standard file transfer protocol*), the imported log will be deleted after it is uploaded to the remote server.

## 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 log file that you want to download, and click *Download* in the toolbar. The *Download Log File* dialog box opens.
3. Select the log file format, either text, Native, or CSV.
4. Select *Compress with gzip* to compress the log file.
5. Click *OK*.

## Log View references

### Chart Builder dialog box

The following settings are available for *Chart Builder* in the tool bar of *Log View* when a log type is selected.

Field	Description
<b>Name</b>	Type a name for the chart.
<b>Columns</b>	Select which columns of data to include in the chart based on the log messages that are displayed on the <i>Log View</i> page.
<b>Group By</b>	Select how to group data in the chart.
<b>Order By</b>	Select how to order data in the chart.
<b>Sort</b>	Select a sort order for data in the chart.
<b>Show Limit</b>	Select a maximum number of log messages to show in the chart.
<b>Device</b>	Displays the device(s) selected on the Log View page.
<b>Time Frame</b>	Displays the time frame selected on the Log View page.
<b>Query</b>	Displays the query being built.
<b>Preview</b>	Displays a preview of the chart.

# System Settings

*System Settings* allows you to manage system options for your FortiAnalyzer unit.



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

## System settings tree menu

You can access the following options by using the tree menu on the *System Settings* pane:

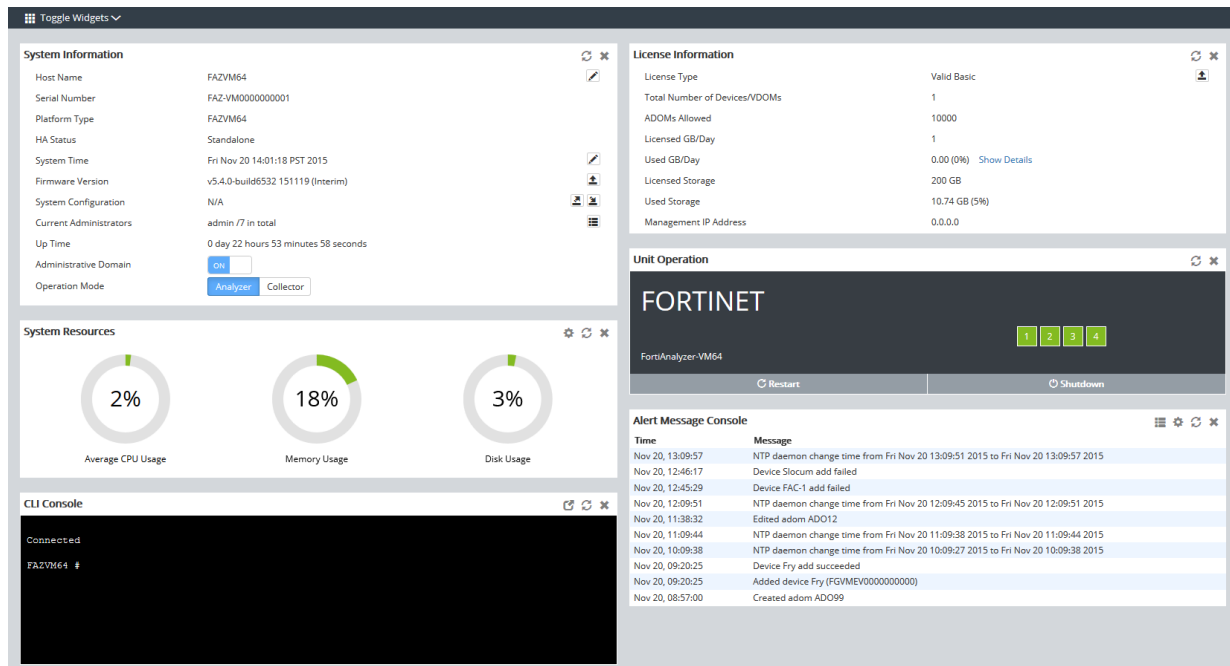
Option	Description
<b>Dashboard</b>	Displays the system settings dashboard. See <a href="#">System settings dashboard on page 152</a> .
<b>All ADOMs</b>	Available when administrative domains (ADOMs) are enabled. You can create, edit, and monitor all ADOMs. See <a href="#">Administrative Domains on page 42</a> .
<b>Storage Info</b>	Displays information about how much FortiAnalyzer disk space has been used for log storage. You can configure and monitor log storage settings. See <a href="#">Storage Info pane on page 88</a> .
<b>Network</b>	Displays the FortiAnalyzer network settings. See <a href="#">Network on page 30</a> .
<b>Admin</b>	Expand and collapse to display and hide access to the following administrator settings for FortiAnalyzer:
<b>Administrators</b>	Displays the administrator accounts. See <a href="#">Administrator Accounts on page 50</a> .
<b>Profile</b>	Displays the administrator profiles. See <a href="#">Administrator profiles on page 54</a> .
<b>Remote Auth Server</b>	Displays the configured remote authorization servers. See <a href="#">Remote authentication servers on page 55</a> .
<b>Admin Settings</b>	Displays the global administrator settings. See <a href="#">Global administrator settings on page 62</a> .
<b>Certificates</b>	Expand and collapse to display and hide access to the following certificate settings:
<b>Local Certificates</b>	View and manage local certificates. See <a href="#">Local Certificates on page 159</a> .

Option	Description
<b>CA Certificates</b>	View and manage CA certificates. See <a href="#">CA Certificates on page 161</a> .
<b>CRL</b>	View and manage Certificate Revocation Lists (CRLs). See <a href="#">Certificate revocation lists on page 162</a> .
<b>Log Forwarding</b>	Displays the log forwarding configurations. See <a href="#">Log Forwarding on page 163</a> .
<b>Fetcher Management</b>	Displays configurations for fetching or receiving logs from another FortiAnalyzer unit. See <a href="#">Log fetcher management on page 167</a> .
<b>Event Log</b>	Displays the event log for FortiAnalyzer. See <a href="#">FortiAnalyzer event log on page 172</a> .
<b>Task Monitor</b>	Displays the task monitor for FortiAnalyzer. See <a href="#">FortiAnalyzer task monitor on page 175</a> .
<b>Advanced</b>	Expand and collapse to display and hide access to the following advanced settings:
<b>SNMP</b>	Displays configured SNMP servers. See <a href="#">SNMP on page 177</a> .
<b>Mail Server</b>	Displays configured mail servers. See <a href="#">Mail servers on page 185</a> .
<b>Syslog Server</b>	Displays configured syslog servers. See <a href="#">Syslog servers on page 186</a> .
<b>Meta Fields</b>	Displays options for meta fields. See <a href="#">Meta fields on page 187</a> .
<b>Device Log Settings</b>	Displays device log settings. See <a href="#">Configuring rolling and uploading of logs on page 83</a> .
<b>File Management</b>	Displays global automatic deletion settings. See <a href="#">Configuring global automatic deletion on page 83</a> .
<b>Advanced Settings</b>	Displays advanced settings, such as changing the ADOM mode, downloading the WSDL file, and specifying the size of the task list. See <a href="#">WSDL files on page 188</a> .

## System settings dashboard

The *Dashboard* contains widgets that provide performance and status information and enable you to configure basic system settings. The dashboard also contains a CLI widget that lets you use the command line through the GUI.





Widget	Description
<b>System Information</b>	Displays basic information about the FortiAnalyzer system, such as up time and firmware version. You can also enable or disable Administrative Domains and adjust the operation mode. From this widget you can manually update the FortiAnalyzer firmware to a different release. For more information, see <a href="#">Viewing and updating FortiAnalyzer firmware on page 159</a> . The widget fields will vary based on how the FortiAnalyzer is configured, for example, if ADOMs are enabled.
<b>System Resources</b>	Displays the real-time and historical usage status of the CPU, memory, and hard disk. For more information, see <a href="#">Viewing CPU status on page 155</a> .
<b>License Information</b>	Displays the devices being managed by the FortiAnalyzer unit and the maximum numbers of devices allowed. For more information, see <a href="#">Viewing license information on page 158</a> . From this widget you can manually upload a license for FortiAnalyzer VM systems.
<b>Unit Operation</b>	Displays status and connection information for the ports of the FortiAnalyzer unit. It also enables you to shutdown and restart the FortiAnalyzer unit or reformat a hard disk. For more information, see <a href="#">Viewing port status on page 155</a> .
<b>CLI Console</b>	Opens a terminal window that enables you to configure the FortiAnalyzer unit using CLI commands directly from the GUI. For more information, see <a href="#">Accessing the CLI on page 158</a> .

Widget	Description
<b>Alert Message Console</b>	Displays log-based alert messages for both the FortiAnalyzer unit itself and connected devices. For more information, see <a href="#">Viewing alert messages on page 155</a> .
<b>Log Receive Monitor</b>	Displays a real-time monitor of logs received. You can select to view data per device or per log type. For more information, see <a href="#">Viewing the number of logs being received on page 156</a> .
<b>Insert Rate vs Receive Rate</b>	<p>Displays the log insert log receive rates in a line graph.</p> <ul style="list-style-type: none"> <li>Log receive rate: how many logs are being received.</li> <li>Log insert rate: how many logs are being actively inserted into the database.</li> </ul> <p>If the log insert rate is higher than the log receive rate, then the database is rebuilding. The lag is the number of logs that are waiting to be inserted. Hover the cursor over a point on the graph to see the exact number of logs that were received and inserted at a specific time. Click the edit icon in the widget toolbar to adjust the time interval shown on the graph (last 1 hour, 8 hours, or 24 hours) and the refresh interval (60 - 240 seconds, 0 to disable).</p>
<b>Log Insert Lag Time</b>	Displays how many seconds the database is behind in processing the logs. Click the edit icon in the widget toolbar to adjust the time and refresh intervals shown on the graph.
<b>Disk I/O</b>	<p>Displays the disk utilization, transaction rate, or throughput as a percentage over time.</p> <p>Click the edit icon in the widget toolbar to select which chart is displayed, the time period shown on the graph (last 1 hour, 8 hours, or 24 hours), and the refresh interval (5 - 240 seconds, 0 to disable) of the chart.</p>

## 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.

Action	Steps
<b>Move a widget</b>	Move the widget by clicking and dragging its title bar, then dropping it in its new location
<b>Add a widgets</b>	Select <i>Toggle Widgets</i> from the toolbar, then select the name widget you need to add.
<b>Delete a widget</b>	Click the <i>Close</i> icon in the widget's title bar.
<b>Reset the dashboard</b>	Select <i>Toggle Widgets &gt; Reset to Default</i> from the toolbar. The dashboards will be reset to the default view.

## Configuring operation modes

The FortiAnalyzer unit has two operation modes: analyzer and collector. For more information, see [Operation modes on page 17](#).

When FortiAnalyzer is operating in collector mode, the SQL database is disabled by default.



Not all FortiAnalyzer models support all operation modes.

### To change the operation mode:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, beside *Operation Mode*, select *Analyzer* or *Collector*, and then select *OK*.

## Viewing port status

The *Unit Operation* widget graphically displays the status of each port. The port name indicates its status by its color. Green indicates that the port is connected. Grey indicates that there is no connection.

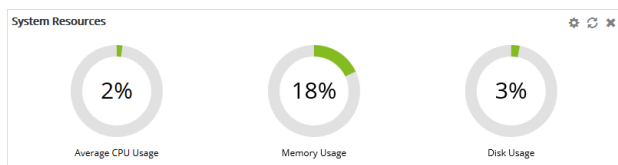
Hover the cursor over the ports to view a pop-up that displays the full name of the interface, the IP address and netmask, the link status, the speed of the interface, and the amounts of sent and received data.

## Viewing CPU status

The *System Resources* widget displays the usage status of the CPUs, memory, and hard disk. You can view system resource information in real-time or historical format, as well as average or individual CPU usage.

To toggle between real-time and historical data, click *Edit* in the widget toolbar, select *Historical* or *Real-time*, edit the other settings as required, then click *OK*.

To view individual CPU usage, from the Real-Time display, click on the CPU chart. To go back to the standard view again, click the chart again.



## Viewing alert messages

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.

Alert Message Console	
Time	Message
Nov 20, 14:10:03	NTP daemon change time from Fri Nov 20 14:09:57 2015 to Fri Nov 20 14:10:03 2015
Nov 20, 13:09:57	NTP daemon change time from Fri Nov 20 13:09:51 2015 to Fri Nov 20 13:09:57 2015
Nov 20, 12:46:17	Device Slocum add failed
Nov 20, 12:45:29	Device FAC-1 add failed
Nov 20, 12:09:51	NTP daemon change time from Fri Nov 20 12:09:45 2015 to Fri Nov 20 12:09:51 2015
Nov 20, 11:38:32	Edited adom ADO12
Nov 20, 11:09:44	NTP daemon change time from Fri Nov 20 11:09:38 2015 to Fri Nov 20 11:09:44 2015
Nov 20, 10:09:38	NTP daemon change time from Fri Nov 20 10:09:27 2015 to Fri Nov 20 10:09:38 2015
Nov 20, 09:20:25	Device Fry add succeeded
Nov 20, 09:20:25	Added device Fry (FGVMEV0000000000)

Click **Edit** from the widget toolbar to view the *Alert Message Console Settings*, where you can adjust the number of entries that are visible in the widget, and the refresh interval.

To view a complete list of alert messages click **Show More** from the widget toolbar. The widget will show the complete list of alerts. To clear the list, click **Delete All Messages**. Click **Show Less** to return to the previous view.

## Viewing the number of logs being received

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

Click **Edit** in the widget toolbar to modify the widget's settings.

Log Receive Monitor Settings

Type

Device

Number of Entries

5

Time Period

Week

Refresh Interval

☒ Enable
 

10

(10 - 240 seconds)

## Setting the date and time

You can either manually set the FortiAnalyzer system time and date, or configure the FortiAnalyzer unit to automatically 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. In the *System Information* widget, find the *System Time* field and click **Edit System Time**.

2. Configure the following settings:

<b>System Time</b>	The date and time according to the FortiAnalyzer unit's clock at the time that this tab was loaded or when you last clicked the <i>Refresh</i> button.
<b>Time Zone</b>	Select the time zone in which the FortiAnalyzer unit is located and whether or not the system automatically adjusts for daylight savings time.
<b>Update Time By</b>	Select <i>Set time</i> to manually set the time, or <i>Synchronize with NTP Server</i> to automatically synchronize the time.
<b>Set Time</b>	Manually set the data and time.
<b>Select Date</b>	Set the date from the calendar or by manually entering it in the format: YYYY/MM/DD.
<b>Select Time</b>	Select the time.
<b>Synchronize with NTP Server</b>	Automatically synchronize the date and time.
<b>Sync Interval</b>	Enter how often, in minutes, that the device should synchronize its time with the NTP server. For example, entering 1440 causes the Fortinet unit to synchronize its time once a day.
<b>Server</b>	Enter the IP address or domain name of an NTP server. Click the plus icon to add more servers. To find an NTP server that you can use, go to <a href="http://www.ntp.org">http://www.ntp.org</a> .

3. Select *OK* to apply your changes.

## 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*.
- It is used in the command prompt of the CLI.
- It is used as the SNMP system name.

The *System Information* widget and the `get system status` CLI command will display the full host name. 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. In the *System Information* widget, find the *Host Name* field and click *Edit Host Name*. The *Host Name* field will become editable.
2. Type in a new host name in the field.  
The host name can be up to 35 characters in length. It can include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.
3. Select *OK* to save the new host name.

## Accessing the CLI

You can enter CLI commands through the GUI, without making a separate Telnet, SSH, or local console connection, using the *CLI Console* widget.



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

For information about the available CLI commands, see the [FortiAnalyzer CLI Reference](#).

When using the *CLI Console* you are logged in under the same administrator account that you used to access the GUI. You can enter commands by typing them, or you can copy and paste commands in to or out of the console.

```

CLI Console
HostName1 #
config      Configure object.
get         Get configuration.
show        Show configuration.
diagnose    Diagnose facility.
execute     Execute static commands.
exit        Exit CLI.
HostName1 #
  
```

Click *Detach* in the widget toolbar to open the widget in a separate window.

## Licenses and firmware

### Viewing license information

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 VM units.

License Information	
License Type	Valid 10UG
Total Number of Devices/VDOMs	18
ADOMs Allowed	10000
Licensed GB/Day	1
Used GB/Day	0.03 (3%) <a href="#">Show Details</a>
Licensed Storage	200 GB
Used Storage	17.29 GB (8%)
Management IP Address	1.1.1.1

## Uploading a FortiAnalyzer VM license

**To upload a FortiAnalyzer VM license:**

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

## Viewing and updating FortiAnalyzer firmware

The version and build numbers of the firmware installed on the FortiAnalyzer unit are listed in the *Firmware Version* field in the *System Information* widget. To take advantage of the latest features and fixes, the device firmware can be updated.

To update the firmware, you must download the latest version from the Customer Service & Support portal at <https://support.fortinet.com>. Click *Update*, then select the firmware image to load from your management computer. For more information, see the [FortiAnalyzer Release Notes](#) in the [Fortinet Document Library](#).

## Local 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.

The FortiAnalyzer has one default local certificate: *Fortinet\_Local*.

## Managing local certificates

You can manage local certificates from the *System Settings > Certificates > Local Certificates* page. Some options are available on the toolbar. Some options are available in the right-click menu.

Option	Description
Create New	Generate a new certificate signing request.
Delete	Delete the selected local certificate or certificates.
Import	Import a certificate.
View Certificate Detail	View details of the selected local certificate.
Download	Download the selected local certificate to the management computer.

## Creating local certificate requests

To create a local certificate request:

1. Go to *System Settings > Certificates > Local Certificates*.
2. Select *Create New* in the toolbar. The *Generate Certificate Signing Request* window opens.
3. Configure the following settings:

<b>Certificate Name</b>	The name of the certificate.
-------------------------	------------------------------

<b>Subject Information</b>	Select and then enter the ID Type ( <i>Host IP</i> , <i>Domain Name</i> , or <i>Email</i> ).
<b>Optional Information</b>	
<b>Organization Unit (OU)</b>	The name of the department. You can enter a series of OUs up to a maximum of 5. To add or remove an OU, use the plus (+) or minus (-) icon.
<b>Organization (O)</b>	Legal name of the company or organization.
<b>Locality (L)</b>	Name of the city or town where the device is installed.
<b>State/Province (ST)</b>	Name of the state or province where the FortiGate unit is installed.
<b>Country (C)</b>	Select the country where the unit is installed from the drop-down list.
<b>E-mail Address (EA)</b>	Contact email address.
<b>Subject Alternative Name</b>	<p>Optionally, enter one or more alternative names for which the certificate is also valid. Separate names with a comma.</p> <p>A name can be:</p> <ul style="list-style-type: none"> <li>• e-mail address</li> <li>• IP address</li> <li>• URI</li> <li>• DNS name (alternatives to the Common Name)</li> <li>• directory name (alternatives to the Distinguished Name)</li> </ul> <p>You must precede the name with the name type.</p>
<b>Key Type</b>	The key type can be <i>RSA</i> or <i>Elliptic Curve</i> .
<b>Key Size</b>	Select the key size from the drop-down list: <i>512 Bit</i> , <i>1024 Bit</i> , <i>1536 Bit</i> , or <i>2048 Bit</i> . Only available when the key type is <i>RSA</i> .
<b>Curve Name</b>	Select the curve name from the drop-down list: <i>secp256r1</i> , <i>secp384r1</i> , or <i>secp521r1</i> . Only available when the key type is <i>Elliptic Curve</i> .
<b>Enrollment Method</b>	The enrollment method is set to <i>File Based</i> .

4. Select **OK** to save the certificate request.. The request is sent and the status is listed as pending.

## Importing local certificates

### To import a local certificate:

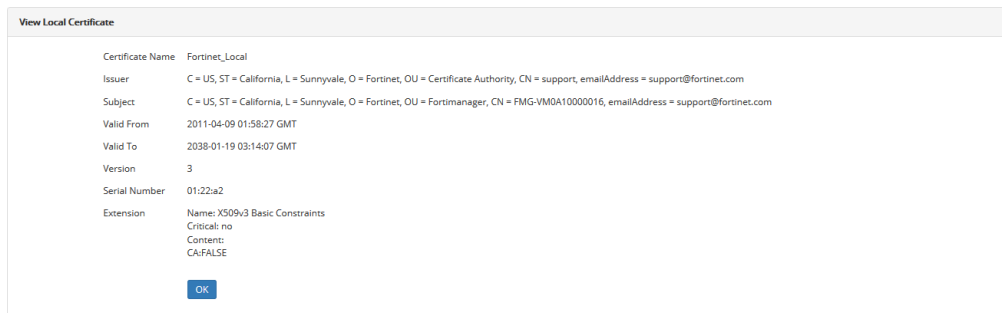
1. Go to **System Settings > Certificates > Local Certificates**.
2. Click **Import** in the toolbar. The **Import** dialog box opens.
3. Click **Browse...** and locate the certificate file on the management computer
4. Select **OK** to import the certificate.



## Viewing details of local certificates

To view details of a local certificate:

1. Go to *System Settings > Certificates > Local Certificates*.
2. Select the certificates that you would like to see details about, then select *View Certificate Detail* in the toolbar. The *Result* page opens.



3. Select *OK* to return to the local certificates list.

## CA Certificates

The FortiAnalyzer has one default CA certificate, Fortinet\_CA. In this sub-menu you can delete, import, view, and download certificates.

## Importing CA certificates

To import a CA certificate:

1. Go to *System Settings > Certificates > CA Certificates*.
2. Select *Import* in the toolbar. The *Import* dialog box opens.
3. Select *Browse...*, browse to the location of the certificate, and select *OK*.

## Viewing CA certificate details

To view a CA certificate's details:

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* in the toolbar. The *Result* page opens.
3. Select *OK* to return to the CA certificates list.

## Downloading CA certificates

### To download a CA certificate:

1. Go to *System Settings > Certificates > CA Certificates*.
2. Select the certificate or certificates that you would like to download, select *Download* in the toolbar, and save the certificate to the management computer.

## Deleting CA certificates

### To delete a CA certificate or certificates:

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

## 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 CRL from the issuing CA.

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

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.

## Importing a CRL

### To import a CRL:

1. Go to *System Settings > Certificates > CRL*.
2. Select *Import* in the toolbar. The *Import* dialog box opens.
3. Select *Browse...*, browse to the location of the CRL, then select *OK* to import it.

## Viewing a CRL

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

## Deleting a CRL

### To delete a CRL or CRLs:

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

## Log Forwarding

You can configure one or more FortiAnalyzer units to forward logs to another FortiAnalyzer unit, a syslog server, or a Common Event Format (CEF) server.

The FortiAnalyzer unit that forwards logs to another unit or server is considered a client, and the FortiAnalyzer unit, syslog server, or CEF server that receives logs is considered a server.

In addition to forwarding logs to another unit or server, the FortiAnalyzer unit that forwards logs retains a local copy of the logs. The local copy of logs are subject to the data policy settings for compressed logs on the FortiAnalyzer unit. See also [Log storage on page 20](#).

## Modes

Log forwarding supports the following modes:

- Real-time  
Logs are forwarded as they are received. With this configuration you can forward logs from a FortiAnalyzer unit to a syslog server or a CEF server.
- Aggregation  
As FortiAnalyzer receives logs, it stores them, and then forwards the logs at a specified time each day. With this configuration, you can forward logs from one or more FortiAnalyzer unit to another FortiAnalyzer unit. Syslog and CEF servers are not supported.
- Combined mode, which uses both real-time and aggregation  
Logs are forwarded as they are received. In addition, archive files are aggregated and forwarded at a specified time each day. With this configuration, you can forward logs from one or more FortiAnalyzer unit to another FortiAnalyzer unit. Syslog and CEF servers are not supported.

## Overview of configuring aggregation mode

This section provides an overview of configuring aggregation mode.

### To configure the server (the FortiAnalyzer unit that receives logs):

1. Define an administrator account that has the *Super\_User* profile assigned to it. See [Defining the user name and password on page 164](#).
2. Enable aggregation in the interface that will receive logs. See [Enabling aggregation on the interface on page 165](#).
3. Enable log aggregation services. See [Enabling the log aggregation service on page 165](#).

### To configure the client (the FortiAnalyzer unit that forwards logs):

1. Go to *System Settings > Log Forwarding*.
2. Click *Create New*. The *Create New Log Forwarding* pane is displayed.
3. In the *Server Name* box, type a name for the log forwarding profile.
4. Beside *Remote Server Type*, select the FortiAnalyzer radio button.
5. In the *Server IP* box, type the IP address of the FortiAnalyzer unit from which you will be receiving logs. In other words, type the IP address of the FortiAnalyzer unit that will forward logs.
6. Select the *Enable Log Aggregation* check box.
7. Type the user name and password for the administrator account that you set up on the server.
8. In the *Upload daily at* list, select when to forward aggregated logs.
9. Click *OK*.

## Overview of configuring combined mode

For the combined mode, follow the configuration instructions for aggregation mode. When you create the log forwarding profile on the client (the FortiAnalyzer unit that forwards logs), select both the *Enable Real-time Forwarding* check box and the *Enable Log Aggregation* check box.

## Enabling log forwarding

Log forwarding is enabled by default in the GUI. If you cannot see *System Settings > Log Forwarding* in the GUI, you must enable it before you can configure it.

### To enable log forwarding:

1. Go to *System Settings > Dashboard*.
2. In the *CLI Console* widget enter the following CLI commands:

```
config system admin setting
  set show-log-forwarding enable
end
```

## Defining the user name and password

When using aggregation mode and the combined mode, both the server and client must use the same username and password.

You must ensure that the server contains an administrator account that is assigned the *Super\_User* profile. When you configure log forwarding on the client, use the username and password that was configured on the server. The user name and password is used to authenticate log forwarding between the server and client.

You can use the default admin account, which is assigned the *Super\_User* profile, or you can create a custom administrator account.

To create an administrator account, see [Configuring administrator accounts on page 52](#).

## Enabling aggregation on the interface

In aggregation mode, you must enable aggregation on the interface that receives logs from clients, such as port 1. You must enable this on the server.

### To enable aggregation on the interface:

1. Go to *System Settings > Network*.
2. Edit the interface that receives logs.
3. Select the *Aggregator* check box, and click *Apply*.

## Enabling the log aggregation service

In aggregation mode, you must enable the aggregation service on the server.

### To enable the log aggregation service:

1. Go to *System Settings > Dashboard*.
2. In the *CLI Console* widget enter the following CLI commands:

```
config system aggregation-service
    set accept-aggregation enable
end
```

## Configuring log forwarding profiles

This section describes how to create log forwarding profiles.

### To configure log forwarding:

1. Go to *System Settings > Log Forwarding*.
2. Click *Create New*. The *Create New Log Forwarding* pane is displayed. For a description of the fields, see [Create New Log Forwarding pane](#).

Create New Log Forwarding

Server Name

Remote Server Type

☒ FortiAnalyzer
☐ Syslog
☐ Comment Event Format(CEF)

Server IP

0.0.0.0

Devices

Select Device +

☒ Enable Real-time Forwarding

Server Port

514

Enable Filters

☒

Log messages that match

☐ All
☒ Any of the Following Conditions

Log Field

Match Criteria

Value

Log Type

Equal to

traffic

+ -

☒ Enable Log Aggregation

User

Password

••••••••

Upload daily at

00:00

OK

Cancel

3. Configure the settings, and click **OK**.

## Managing log forwarding

You can manage log forwarding from the *System Settings > Log Forwarding* pane. Some options are available in the menu on the toolbar. Some options are available in the right-click menu. Right-click a log forwarding configuration to display the menu.

Option	Description
<b>Create New</b>	Create a new log forwarding configuration.
<b>Edit</b>	Edit the selected log forwarding configuration.
<b>Delete</b>	Delete the selected log forwarding configuration.
<b>Aggregation Now</b>	Send the batched logs to the remote server now instead of waiting for the scheduled time.

## Create New Log Forwarding pane

The following fields are available on the *Add Log Forwarding* pane:

<b>Server Name</b>	Enter a name to identify the log forwarding configuration.
<b>Remote Server Type</b>	Select the type of destination to which you are forwarding logs. Select one of the following: <i>FortiAnalyzer</i> , <i>Syslog</i> , <i>Common Event Format (CEF)</i> . The destination is considered the aggregation server that receives the logs.
<b>Server IP</b>	Enter the IP address for the server that will receive the logs.

<b>Devices</b>	Select <i>Select Devices</i> to select the devices for which you want to forward logs. Select devices then select <i>OK</i> to add the devices.
<b>Enable Real-Time Forwarding</b>	Select to forward logs to the aggregation server as the FortiAnalyzer client receives the logs.
<b>Server Port</b>	Enter the server port. The default port is 514.
<b>Enable Filters</b>	Select to forward logs in real-time based on filters. You can only enable filters when <i>Enable Real-Time Forwarding</i> is selected.
<b>Log messages that match</b>	Select <i>All</i> to forward all log messages, or select <i>Any of the Following Conditions</i> to forward only log messages that meet the requirements of the specified filters.
<b>Add Filter</b>	Select the <i>Add Filter</i> icon to specify a filter by completing the <i>Log Field</i> , <i>Match Criteria</i> , and <i>Value</i> options. Click the <i>X</i> icon to delete a filter.
<b>Enable Log Aggregation</b>	Select to batch logs, and then send the logs to the aggregation server at a specified time. This option is available only when <i>Remote Server Type</i> is set to <i>FortiAnalyzer</i> .
<b>User</b>	Enter the user name for the aggregation server that is receiving logs. The user must be defined in an administrator account on the aggregation server that has the <i>Super_User</i> profile assigned to it.
<b>Password</b>	Enter the password for the aggregation server that is receiving logs. The password must be defined in an administrator account on the aggregation server that has the <i>Super_User</i> profile assigned to it. You must also set the same password on the client by using the following CLI command: <code>config system aggregation-service</code> . The password is used when the server and client are communicating during log aggregation.
<b>Upload Daily at</b>	Specify what time to upload the batched logs to the remove server. Select a time from the drop-down list.

## Log fetcher management

You can fetch compressed logs and make them indexed logs. Indexed logs support data analysis on the *FortiView* tab and the *Reports* tab. See also [Compressed logs and indexed logs on page 20](#).

You must fetch logs from one FortiAnalyzer device to a second FortiAnalyzer device. You cannot fetch logs by using only one FortiAnalyzer device. One FortiAnalyzer device operates as a fetch client, and a second FortiAnalyzer device operates as a fetch server.

On the fetch client, you can send a request to the fetch server for logs from a range of time. On the fetch server, you can approve or deny the request. When the request is approved, the fetch server gathers the requested logs into a compressed file and transfers the compressed file to the fetch client. When the fetch client receives the

logs, the logs are automatically indexed in the SQL database. You can analyze the indexed logs by using the *FortiView* tab and the *Reports* tab.

Each FortiAnalyzer device can perform either a fetch server role or a fetch client role, and each FortiAnalyzer device can perform only one role at a time. A maximum of one transfer between two FortiAnalyzer devices can be performed at one time.

Following is a summary of the fetch client and fetch server roles:

Local Device Role	Purpose
Fetch client	Request permission to fetch logs from a FortiAnalyzer device that is operating as a fetch server. When the fetched logs arrive on the fetch client, the logs are automatically inserted into the SQL database to support data analysis. The data policy for the fetch client applies to fetched logs.
Fetch server	Approve or reject client requests to retrieve logs from the FortiAnalyzer device. When the request is approved, the fetch server gathers the requested logs into a compressed file and transfers the compressed file to the fetch client. The process of gathering and transferring logs happens in the background on the fetch server.

## Overview of fetching logs

You must perform several steps to fetch logs. Following is an overview of the steps.

### To fetch logs:

1. On the fetch client, prepare to fetch logs. See [Preparing to fetch logs on page 168](#).
2. On the fetch server, create a fetch server profile. See [Configuring fetch server profiles on page 169](#).
3. On the fetch client, create a fetch client profile. See [Configuring fetch client profiles on page 169](#).
4. On the fetch client, send a request to fetch logs. See [Sending requests to fetch logs on page 169](#).
5. On the fetch server, approve or reject the request to fetch logs. See [Approving or rejecting requests to fetch logs on page 170](#).
6. Monitor the fetch process. See [Monitoring request sessions on page 170](#).
7. On the fetch client, view data analysis of fetched logs by using the *FortiView* tab and the *Reports* tab.

## Preparing to fetch logs

Before you can fetch logs, you must ensure that the FortiAnalyzer device can successfully fetch logs and retain them long enough to allow you to analyze data.

### To send a request to fetch logs:

1. On the fetch server, identify the device for which you want to fetch logs and the time range for the logs that you want to fetch.
2. On the fetch client, add the device for which you want to fetch logs.



Alternately you can import the device, which also imports the ADOM for the device into the GUI. Before you can import a device, you must first enable the feature by using the `show-device-import-export` command in the CLI.

3. On the fetch client, ensure that the ADOM for the device has enough available space for the logs that you will fetch.
4. On the fetch client, ensure that the data policy for the ADOM includes a date range that spans the date range for the logs that you will fetch.

For example, today is June 1, and the data policy keeps indexed logs for 30 days (May 1 - May 30). You want to fetch logs for April 1 - 8. Ensure that the data policy for the ADOM retains indexed and compressed logs for at least 62 days, which covers 31 days (May) + 30 days (April) + 1 day (June 1). Otherwise, the fetched logs will be automatically deleted after you fetch them.

## Configuring fetch server profiles

A fetch request requires a fetch server profile and a fetch client profile with matching user and password fields. This procedure describes how to create a fetch server profile.

### To configure fetch server profiles:

1. On the fetch server, go to *System Settings > Advanced > Fetcher Management*.
2. On the *Profiles* tab, select *Create New*.
3. Complete the options, and click *OK*. For a description of the options, see [Create New dialog box on page 171](#). The fetch server profile is created.

## Configuring fetch client profiles

A fetch request requires a fetch server profile and a fetch client profile with matching user and password fields. This procedure describes how to create a fetch client profile.

### To configure fetch client profiles:

1. On the fetch client, go to *System Settings > Advanced > Fetcher Management*.
2. On the *Profiles* tab, select *Create New*. The *Create New* dialog box is displayed.
3. Complete the options, and select *OK*. For a description of the options, see [Create New dialog box on page 171](#). The fetch client profile is created.

## Sending requests to fetch logs

A fetch client requests approval from a fetch server to fetch logs.

### To send a request to fetch logs:

1. On the fetch client, go to *System Settings > Advanced > Fetcher Management*.
2. On the *Profiles* tab, select *Fetch*. The *Fetch Logs* dialog box is displayed.
3. Complete the options. For a description of the options, see [Fetch Logs dialog box on page 171](#).
4. Select *Fetch Now*. The fetch request is sent to the fetch server.

## Approving or rejecting requests to fetch logs

You can approve or reject a client request to fetch logs. When you approve the request, the process of retrieving the compressed logs occurs in the background.

### To approve or reject requests to fetch logs:

1. On the fetch server, go to the *System Settings > Advanced > Fetcher Management*.
2. Select the *Received Sessions* tab. The list of requests to fetch logs is displayed.
3. For each request, hover the mouse over the *Profile* icon to view details about the request.
4. For each request, select *Approve* to allow the client to fetch logs, or select *Reject* to deny the client request to fetch logs.

## Monitoring request sessions

You can monitor the fetch request sessions as follows on the *System Settings > Advanced > Fetcher Management* pane:

- On a fetch client, you can monitor fetch request on the *Sent Sessions* tab.
- On a fetch server, you can monitor fetch request on the *Received Sessions* tab.

While a session for fetching logs is in progress, you can view the status of the transfer. You can also pause, resume, and cancel the session as follows:

- On the fetch client, you can pause and resume a session on the *Sent Sessions* tab.
- On the fetch server, you can cancel a session on the *Received Sessions* tab.

When a session has finished fetching logs, the status displays *Done*. The status indicates that the logs have been transferred from the server to the client, but not yet inserted into the SQL database. There is no status indicator for when the logs have been inserted the SQL database. You must continue to check the *FortiView* tab to discover when the logs have been inserted into the database.

## Managing fetch profiles

You can manage fetch profiles by using the *System Settings > Advanced > Fetcher Management > Profiles* page. The options are available as buttons on the toolbar.

Option	Description
Create New	Create a new fetch profile.
Edit	Edit the selected fetch profile.
Delete	Delete the selected fetch profile.

## Fetcher Management references

### Create New dialog box

Option	Description
<b>Name</b>	Type a name for the profile.
<b>IP Address</b>	Type the IP address for the FortiAnalyzer device from which you want to retrieve logs. The FortiAnalyzer device will operate as a fetch server. Available only when you create a fetch client profile.
<b>User</b>	Type a user name for the profile. The user name must be the same for the fetch server profile and the fetch client profile to allow the profiles to communicate. The user name is unrelated to the login to the FortiAnalyzer unit. The user name is used only for the fetch session.
<b>Password</b>	Type a password for the profile. The password must be the same for the fetch server profile and the fetch client profile to allow the profiles to communicate. The password is unrelated to the login for the FortiAnalyzer unit. The password is used only for the fetch session.

### Fetch Logs dialog box

Option	Description
<b>Name</b>	Displays the name of the fetch client profile.
<b>Server IP</b>	Displays the name of the FortiAnalyzer device that is operating as a fetch server from which the client will fetch logs.
<b>User</b>	Displays the user name for the session.
<b>Devices</b>	You can narrow the scope of logs to fetch on the FortiAnalyzer device that is operating as a fetch server by using device filters. Each filter includes the following fields: ADOM, Device ID, VDOM.
<b>Add Device Filter</b>	Select to add a new device filter to the table.
<b>ADOM</b>	Specify the ADOMs from which to fetch logs. Type * for all ADOMs, or type the name of a specific ADOM. You can also use partial wildcards in the format of <keyword>*, for example, adom*.
<b>Device ID</b>	Specify the ID for the device from which to fetch logs. Type * for all device IDs, or type the ID of a specific device. You can also use partial wildcards in the format of <keyword>*, for example, fgt*.

Option	Description
<b>VDOM</b>	Specify the VDOM for the device from which to fetch logs. Type * for all VDOMs, or type the name of a specific VDOM.
<b>Enable Filters</b>	Select to enable log-message filters. You can specify what types of log messages to fetch by adding multiple filters.
<b>Time Period</b>	Specify what time range of log messages to fetch. You must ensure that the data policy on the fetch client includes a time range that spans the time requested in the <i>Time Period</i> option.
<b>Index Fetch Logs</b>	Select to automatically index fetched logs in the SQL database on the fetch client.
<b>Secure Connect</b>	Select to transfer fetched logs from the server to the client by using SSL connection.
<b>Fetch Now</b>	Select to send the fetch request to the server.
<b>Save</b>	Select to save the changes without sending the fetch request.

## FortiAnalyzer event log

The logs created by Fortinet are viewable within the GUI. 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 GUI 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.

Refresh						Download	Raw Log	Historical Log
#	Date Time	Level	User	Sub Type	Message			
1	2015-11-20 16:24:05	warning	system	FortiAnalyzer event	Device[FGVMEV0000000000] did not receive any log in last 1516 minutes.			
2	2015-11-20 16:19:03	warning	system	FortiAnalyzer event	Device[FGVMEV0000000000] did not receive any log in last 1511 minutes.			
3	2015-11-20 16:14:02	warning	system	FortiAnalyzer event	Device[FGVMEV0000000000] did not receive any log in last 1506 minutes.			
4	2015-11-20 16:10:49	information	admin-jconsole(172.172.172.111)	System manager event	user 'admin' with profile 'Super_User' timed out from jconsole(172.172.172.111)			
5	2015-11-20 16:10:48	information	admin-GUI(172.172.172.111)	System manager event	The session of the user 'admin' from jconsole(172.172.172.111) is killed			
6	2015-11-20 16:10:48	information	admin-jconsole(172.172.172.111)	System manager event	user 'admin' with profile 'Super_User' login accepted from jconsole(172.172.172.111)			
7	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.key=admin,act=edit,			
8	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.dashboard,key=admin,act=add,name=Insert Rate vs Receive Rate,column=2,refresh-interval=60,tabid=1,widget-type=logdb-perf,time-period=8hour			
9	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.dashboard,key=admin,act=edit,			
10	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.dashboard,key=admin,act=add,name=Alert Message Console,column=2,refresh-interval=10,tabid=1,widget-type=alert,num-entries=25			
11	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.key=admin,act=edit,			
12	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.dashboard,key=admin,act=add,name=Unit Operation,column=2,refresh-interval=0,tabid=1,widget-type=sysop			
13	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.key=admin,act=edit,			
14	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.dashboard,key=admin,act=add,name=License Information,column=2,refresh-interval=0,tabid=1,widget-type=licinfo			
15	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.key=admin,act=edit,			
16	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.dashboard,key=admin,act=add,name=Log Insert Lag Time,column=1,refresh-interval=60,tabid=1,widget-type=logdb.lag,time-period=8hour			
17	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.key=admin,act=edit,			
18	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.dashboard,key=admin,act=add,name=Log Receive Monitor,column=1,refresh-interval=10,tabid=1,widget-type=top-lograte,log-rate-type=log-log-rate-period=6hours			
19	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.key=admin,act=edit,			
20	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.dashboard,key=admin,act=add,name=CLI Console,column=1,refresh-interval=0,tabid=1,widget-type=jsconsole			
21	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.key=admin,act=edit,			
22	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.dashboard,key=admin,act=add,name=System Resources,column=1,refresh-interval=10,tabid=1,widget-type=sysres,res-view-type=real-time/_res-period=hour/_res-cpu-display=each			
23	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.key=admin,act=edit,			
24	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.dashboard,key=admin,act=add,name=System Information,column=1,refresh-interval=0,tabid=1,widget-type=sysinfo			
25	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.key=admin,act=edit,			
26	2015-11-20 16:10:43	notice	admin-GUI(172.172.172.111)	System manager event	path=system.admin.user.dashboard,act=clear			
27	2015-11-20 16:10:39	notice	admin-GUI(172.172.172.111)	System manager event	path=system.global,act=edit,hostname=HostName1(FA2VM64)			
28	2015-11-20 16:10:39	notice	admin-GUI(172.172.172.111)	System manager event	hostname changed: FA2VM64->agt: HostName1			
29	2015-11-20 16:10:18	information	admin-jconsole(172.172.172.111)	System manager event	user 'admin' with profile 'Super_User' login accepted from jconsole(172.172.172.111)			
30	2015-11-20 16:10:15	warning	ntp_daemon-system	System manager event	NTP daemon change time from Fri Nov 20 16:10:09 2015 to Fri Nov 20 16:10:15 2015			
31	2015-11-20 16:09:00	warning	system	FortiAnalyzer event	Device[FGVMEV0000000000] did not receive any log in last 1501 minutes.			
32	2015-11-20 16:03:59	warning	system	FortiAnalyzer event	Device[FGVMEV0000000000] did not receive any log in last 1496 minutes.			
33	2015-11-20 16:00:10	information	admin-jconsole(172.172.172.107)	System manager event	user 'admin' with profile 'Super_User' login accepted from jconsole(172.172.172.107)			
34	2015-11-20 15:58:58	warning	system	FortiAnalyzer event	Device[FGVMEV0000000000] did not receive any log in last 1491 minutes.			
35	2015-11-20 15:53:56	warning	system	FortiAnalyzer event	Device[FGVMEV0000000000] did not receive any log in last 1486 minutes.			
36	2015-11-20 15:48:55	warning	system	FortiAnalyzer event	Device[FGVMEV0000000000] did not receive any log in last 1481 minutes.			

The following information is displayed:

#	The log number.
Date Time	The date and time that the log file was generated.
Level	The log level: <ul style="list-style-type: none"> <li>• Debug</li> <li>• Information</li> <li>• Notification</li> <li>• Warning</li> <li>• Error</li> <li>• Critical</li> <li>• Alert</li> <li>• Emergency</li> </ul>
User	User information.

<b>Sub Type</b>	The log sub-type:	
	System manager event	HA event
	FG-FM protocol event	Firmware manager event
	Device configuration event	FortiGuard service event
	Global database event	FortiClient manager event
	Script manager event	FortiMail manager event
	Web portal event	Debug I/O log event
	Firewall objects event	Configuration change event
	Policy console event	Device manager event
	VPN console event	Web service event
	Endpoint manager event	FortiAnalyzer event
	Revision history event	Log daemon event
	Deployment manager event	FIPS-CC event
	Real-time monitor event	Managed devices event
	Log and report manager event	
<b>Message</b>	Log message details.	

The following options are available:

<b>Add Filter</b>	Filter the event log list based on the log level, user, sub type, or message.
<b>Download</b>	Download the event logs in either CSV or the normal format.
<b>Raw Log / Formatted Log</b>	Click on <i>Raw Log</i> to view the logs in their raw state. Click <i>Formatted Log</i> to view them in the formatted into a table.
<b>Historical Log</b>	Click to view the historical logs list.
<b>View</b>	View the selected log file. This option is only available when viewing historical event logs.
<b>Delete</b>	Delete the selected log file. This option is only available when viewing historical event logs.

<b>Clear</b>	Clear the selected file of logs. This option is only available when viewing historical event logs.
<b>Type</b>	<p>Select the type from the drop down list. This option is only available when viewing historical logs.</p> <p>Select one of the following: <i>Event Log</i>, <i>FDS Upload Log</i>, or <i>FDS Download Log</i>.</p> <ul style="list-style-type: none"> <li>• <i>FDS Upload Log</i>: Select the device from the drop-down list.</li> <li>• <i>FDS Download Log</i>: Select the service (<i>FDS</i>, or <i>FCT</i>) from the <i>Service</i> drop-down list, select the event type (<i>All Event</i>, <i>Push Update</i>, <i>Poll Update</i>, or <i>Manual Update</i>) from the <i>Event</i> drop-down list, and then click <i>Go</i> to browse logs.</li> </ul>
<b>Search</b>	Enter a search term to search the historical logs. This option is only available when viewing historical event logs.
<b>Pagination</b>	Use these page options to browse logs and adjust how many logs are shown per page.

## FortiAnalyzer task monitor

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

### Viewing tasks performed for the FortiAnalyzer unit

Go to *System Settings > Task Monitor*, then select a task category in the *View* field. Select the history icon for task details.

Delete: View: All							
<input type="checkbox"/>	ID	Source	Description	User	Status	Start Time	ADOM
<input type="checkbox"/>	19	Device Manager	Add/delete Unregistered Devices	admin		Fri Nov 13 15:53:54 2015	root
<input type="checkbox"/>	18	Device Manager	Add Device	admin		Thu Nov 12 15:53:42 2015	root
<input type="checkbox"/>	17	Device Manager	Add/delete Unregistered Devices	admin		Thu Nov 12 15:02:30 2015	root
<input type="checkbox"/>	16	Device Manager	Add/delete Unregistered Devices	admin		Thu Nov 12 15:02:00 2015	root
<input type="checkbox"/>	15	Device Manager	Add/delete Unregistered Devices	admin		Wed Sep 2 09:08:56 2015	root
<input type="checkbox"/>	14	Device Manager	Delete Device	admin		Wed Sep 2 09:08:06 2015	root
<input type="checkbox"/>	13	Device Manager	Add/delete Unregistered Devices	admin		Wed Sep 2 09:01:14 2015	root
<input type="checkbox"/>	12	Device Manager	Add/delete Unregistered Devices	admin		Tue Sep 1 17:23:35 2015	root
<input type="checkbox"/>	11	Device Manager	Delete Device	admin		Tue Sep 1 17:22:26 2015	root
<input type="checkbox"/>	10	Device Manager	Add/delete Unregistered Devices	admin		Tue Sep 1 17:21:33 2015	root
<input type="checkbox"/>	9	Device Manager	Add/delete Unregistered Devices	admin		Tue Sep 1 17:21:18 2015	FortiManager
<input type="checkbox"/>	8	Device Manager	Add/delete Unregistered Devices	admin	<div><div></div>1%</div>	Fri Jul 31 15:40:40 2015	root
<input type="checkbox"/>	7	Device Manager	Add/delete Unregistered Devices	admin	<div><div></div>1%</div>	Fri Jul 31 15:39:20 2015	root
<input type="checkbox"/>	6	Device Manager	Add Device	admin		Fri Jul 31 15:38:15 2015	root
<input type="checkbox"/>	5	Device Manager	Add/delete Unregistered Devices	admin		Mon Jul 27 11:26:04 2015	root
<input type="checkbox"/>	4	Device Manager	Delete Device	admin		Thu Jul 23 09:52:09 2015	root
<input type="checkbox"/>	3	Device Manager	Delete Device	admin		Sat Jul 4 21:11:07 2015	root
<input type="checkbox"/>	2	Device Manager	Delete Device	admin		Sat Jul 4 21:10:45 2015	root
<input checked="" type="checkbox"/>	1	Device Manager	Add/delete Unregistered Devices	admin		Tue Jun 30 22:07:50 2015	root

< prev 1 next > (1 of 1)

Total:3 Pending:0 In Progress:0 Completed ( Success:3 Warning:0 Error:0 )

1	FGT1KC0000000007	33.3.3.3		Checking device status	
2	FGT1KC6666666666	22.2.2.2		Checking device status	
3	v7a	11.1.111.11		Checking device status	

< prev 1 next > (1 of 1)

The following information is available:

<b>ID</b>	The identification number for a task.
<b>Source</b>	The platform from where the task is performed. Click the expand arrow to view details of the specific task and access the history button.
<b>Description</b>	The nature of the task. Click the arrow to display the specific actions taken under this task.
<b>User</b>	The user or users who performed the tasks.
<b>Status</b>	<p>The status of the task (hover over the icon to view the description):</p> <ul style="list-style-type: none"> <li>• <i>Done</i>: Completed with success.</li> <li>• <i>Error</i>: Completed without success.</li> <li>• <i>Canceled</i>: User canceled the task.</li> <li>• <i>Canceling</i>: User is canceling the task.</li> <li>• <i>Aborted</i>: The FortiAnalyzer system stopped performing this task.</li> <li>• <i>Aborting</i>: The FortiAnalyzer system is stopping performing this task.</li> <li>• <i>Running</i>: Being processed. In this status, a percentage bar appears in the Status column.</li> <li>• <i>Pending</i></li> <li>• <i>Warning</i></li> </ul>
<b>Start Time</b>	The time that the task was started.
<b>ADOM</b>	The ADOM associated with the task.
<b>History</b>	Click the history button to view task details.

## Deleting tasks

You can remove a selected task or tasks from the list. Select the task or tasks, click *Delete* in the toolbar, then click *OK* in the confirmation dialog box.

## Filtering the task view

You can select which tasks to view from the drop-down list, based on their status. Select one of the following: *Running*, *Pending*, *Done*, *Error*, *Canceling*, *Canceled*, *Aborting*, *Aborted*, *Warning*, or *All*.

## Configuring the task list size

To configure the task list size:

1. Go to *System Settings > Advanced > Advanced Settings*.
2. In the *Task List Size* field, type the maximum number of tasks to retain, then select *Apply*.



## SNMP

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

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

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

SNMP has two parts:

1. The SNMP agent or the device that is sending traps, and
2. The SNMP manager that monitors those traps.

The SNMP communities on the monitored FortiGate devices are hard coded and configured by the FortiAnalyzer system - they are not user configurable.

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

## Configuring an SNMP agent

An 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* to configure the SNMP agent.

SNMP

SNMP Agent

☒ Enable

Description

Location

Contact

Apply

SNMP v1/v2c

+ Create New

☒ Edit

☐ Delete

<input type="checkbox"/> Community Name	Queries	Traps	Enable
<input type="checkbox"/> Solara	✓	✓	<input checked="" type="checkbox"/>
<input type="checkbox"/> Terminus	✓	✓	<input checked="" type="checkbox"/>
<input type="checkbox"/> Trantor	✓	✓	<input checked="" type="checkbox"/>

SNMP v3

+ Create New

☒ Edit

☐ Delete

<input type="checkbox"/> User Name	Security Level	Notification Hosts	Queries
<input type="checkbox"/> Bliss	No Authentication, No Privacy		<input type="checkbox"/>
<input type="checkbox"/> Daneel	Authentication, No Privacy		<input type="checkbox"/>
<input type="checkbox"/> Fallom	Authentication, Privacy		<input type="checkbox"/>
<input type="checkbox"/> Golan	No Authentication, No Privacy		<input type="checkbox"/>

The following information and options are available:

<b>SNMP Agent</b>	Select to enable the FortiAnalyzer SNMP agent. When this is enabled, it sends FortiAnalyzer SNMP traps.
<b>Description</b>	Type a description of this FortiAnalyzer system to help uniquely identify this unit.
<b>Location</b>	Type the location of this FortiAnalyzer system to help find it in the event it requires attention.
<b>Contact</b>	Type the contact information for the person in charge of this FortiAnalyzer system.
<b>SNMP v1/2c</b>	The list of SNMP v1/v2c communities added to the FortiAnalyzer configuration.
<b>Create New</b>	Click <i>Create New</i> to add a new SNMP community. For more information, see <a href="#">Configuring an SNMP v1/v2c community on page 179</a> .
<b>Edit</b>	Edit the selected SNMP community.
<b>Delete</b>	Remove the selected SNMP community.
<b>Search</b>	Search the SNMP communities.
<b>Community Name</b>	The name of the SNMP community.
<b>Queries</b>	The status of SNMP queries for each SNMP community. The enabled icon indicates that at least one query is enabled. The disabled icon indicates that all queries are disabled.
<b>Traps</b>	The status of SNMP traps for each SNMP community. The enabled icon indicates that at least one trap is enabled. The disabled icon indicates that all traps are disabled.
<b>Enable</b>	Select to enable or deselect to disable the SNMP community.
<b>SNMP v3</b>	The list of SNMPv3 users added to the FortiAnalyzer configuration.
<b>Create New</b>	Select <i>Create New</i> to add a new SNMP community. For more information, see <a href="#">Configuring a SNMPv3 user on page 181</a> .
<b>Edit</b>	Edit the selected SNMP user.
<b>Delete</b>	Remove the selected SNMP user.
<b>Search</b>	Search the SNMP users.

<b>User Name</b>	The user name for the SNMPv3 user.
<b>Security Level</b>	The security level assigned to the SNMPv3 user.
<b>Notification Hosts</b>	The notification host or hosts assigned to the SNMPv3 user.
<b>Queries</b>	The status of SNMP queries for each SNMP user. The enabled icon indicates that query is enabled. The disabled icon indicates query is disabled.

### Configuring an SNMP v1/v2c community

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



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

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

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

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

**New SNMP Community**

Name:

Hosts:

IP Address/Netmask	Interface	Delete
<input type="button" value="Add"/>		

Queries:

Protocol	Port	Enable
v1	<input type="text" value="161"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="161"/>	<input checked="" type="checkbox"/>

Traps:

Protocol	Port	Enable
v1	<input type="text" value="162"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="162"/>	<input checked="" type="checkbox"/>

SNMP Event	Enable
Interface IP changed	<input checked="" type="checkbox"/>
Log Disk Space Low	<input checked="" type="checkbox"/>
CPU Overuse	<input checked="" type="checkbox"/>
Memory Low	<input checked="" type="checkbox"/>
System Restart	<input checked="" type="checkbox"/>
CPU usage exclude NICE threshold	<input checked="" type="checkbox"/>
RAID Event	<input checked="" type="checkbox"/>
High licensed log GB/day	<input checked="" type="checkbox"/>
Log Alert	<input checked="" type="checkbox"/>
Log Rate	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="checkbox"/>

Configure the following settings:

<b>Name</b>	Type a name to identify the SNMP community. If you are editing an existing community, you will be unable to change the name.
<b>Hosts</b>	The list of hosts that can use the settings in this SNMP community to monitor the FortiAnalyzer system. Select <i>Add</i> to create a new entry that you can edit.
<b>IP Address</b>	Type the IP address of an SNMP manager. By default, the IP address is 0.0.0.0 so that any SNMP manager can use this SNMP community.
<b>Interface</b>	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.
<b>Delete</b>	Select the delete icon to remove this SNMP manager entry.
<b>Add</b>	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.
<b>Queries</b>	Type the port number (161 by default) that the FortiAnalyzer system uses to send v1 and v2c queries to the FortiAnalyzer in this community. Enable queries for each SNMP version that the FortiAnalyzer system uses.

**Traps**

Type the Remote port number (162 by default) that the FortiAnalyzer system uses to send v1 and v2c traps to the FortiAnalyzer in this community. Enable traps for each SNMP version that the FortiAnalyzer system uses.

**SNMP Event**

Enable the events that will cause the FortiAnalyzer unit to send SNMP traps to the community:

- Interface IP changed
- Log Disk Space Low
- CPU Overuse
- Memory Low
- System Restart
- CPU usage exclude NICE threshold
- RAID Event (only available for devices which support RAID)
- High licensed device quota
- High licensed log GB/day
- Log Alert
- Log Rate
- Data Rate

## Configuring a SNMPv3 user

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

**New SNMP User**

User Name:

Security Level:

Authentication Algorithm:  Password:

Private Algorithm:  Password:

Queries: ☐ Enable Port:

Notification Hosts:

SNMP Event	Enable
Interface IP changed	<input checked="" type="checkbox"/>
Log Disk Space Low	<input checked="" type="checkbox"/>
CPU Overuse	<input checked="" type="checkbox"/>
Memory Low	<input checked="" type="checkbox"/>
System Restart	<input checked="" type="checkbox"/>
CPU usage exclude NICE threshold	<input checked="" type="checkbox"/>
RAID Event	<input checked="" type="checkbox"/>
High licensed log GB/day	<input checked="" type="checkbox"/>
Log Alert	<input checked="" type="checkbox"/>
Log Rate	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="checkbox"/>

Configure the following settings:

**User Name**

The name of the SNMPv3 user.

<b>Security Level</b>	<p>The security level of the user. Select one of the following:</p> <ul style="list-style-type: none"> <li>• <i>No Authentication, No Privacy</i></li> <li>• <i>Authentication, No Privacy</i>: Select the authentication algorithm (SHA1, MD5) and enter the password.</li> <li>• <i>Authentication, Privacy</i>: Select the authentication algorithm (SHA1, MD5), the private algorithm (AES, DES), and enter the password.</li> </ul>
<b>Queries</b>	Select to enable queries then enter the port number. The default port is 161.
<b>Notification Hosts</b>	The IP address or addresses of the host. Click the add icon to add multiple IP addresses.
<b>SNMP Event</b>	<p>Enable the events that will cause the FortiAnalyzer unit to send SNMP traps to the community.</p> <p>FortiAnalyzer SNMP events:</p> <ul style="list-style-type: none"> <li>• Interface IP changed</li> <li>• Log disk space low</li> <li>• CPU Overuse</li> <li>• Memory Low</li> <li>• System Restart</li> <li>• CPU usage exclude NICE threshold</li> <li>• RAID Event (only available for devices which support RAID)</li> <li>• High licensed device quota</li> <li>• High licensed log GB/day</li> <li>• Log Alert</li> <li>• Log Rate</li> <li>• Data Rate</li> </ul>

## SNMP MIBs

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

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

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

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

You can download the FortiAnalyzer MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiAnalyzer 5.00 file folder. See [Appendix C - SNMP MIB Support on page 194](#).

MIB file name or RFC	Description
<b>FORTINET-CORE-MIB.mib</b>	The proprietary Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor Fortinet unit configuration settings and receive traps from the Fortinet SNMP agent.
<b>FORTINET-FORTIMANAGER-MIB.mib</b>	The proprietary FortiAnalyzer MIB includes system information and trap information for FortiAnalyzer units.
<b>RFC-1213 (MIB II)</b>	<p>The Fortinet SNMP agent supports MIB II groups with the following exceptions.</p> <ul style="list-style-type: none"> <li>No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10).</li> <li>Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all Fortinet traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB.</li> </ul>
<b>RFC-2665 (Ethernet-like MIB)</b>	<p>The Fortinet SNMP agent supports Ethernet-like MIB information with the following exception.</p> <p>No support for the dot3Tests and dot3Errors groups.</p>

## SNMP traps

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

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

Trap message	Description
<b>ColdStart, WarmStart, LinkUp, LinkDown</b>	Standard traps as described in RFC 1215.
<b>CPU usage high (fnTrapCpuThreshold)</b>	<p>CPU usage exceeds the set percent. This threshold can be set in the CLI using the following commands:</p> <pre>config system snmp sysinfo     set trap-high-cpu-threshold &lt;percentage value&gt; end</pre>
<b>CPU usage excluding NICE processes (fmSysCpuUsageExcludedNice)</b>	<p>CPU usage excluding NICE processes exceeds the set percentage. This threshold can be set in the CLI using the following commands:</p> <pre>config system snmp sysinfo     set trap-cpu-high-exclude-nice-threshold &lt;percentage value&gt; end</pre>

Trap message	Description
<b>Memory low</b> (fnTrapMemThreshold)	Memory usage exceeds 90 percent. This threshold can be set in the CLI using the following commands: <pre>config system snmp sysinfo   set trap-low-memory-threshold &lt;percentage value&gt; end</pre>
<b>Log disk too full</b> (fnTrapLogDiskThreshold)	Log disk usage has exceeded the configured threshold. Only available on devices with log disks.
<b>Temperature too high</b> (fnTrapTempHigh)	A temperature sensor on the device has exceeded its threshold. Not all devices have thermal sensors. See manual for specifications.
<b>Voltage outside acceptable range</b> (fnTrapVoltageOutOfRange)	Power levels have fluctuated outside of normal levels. Not all devices have voltage monitoring instrumentation.
<b>Power supply failure</b> (fnTrapPowerSupplyFailure)	Power supply failure detected. Not available on all models. Available on some devices which support redundant power supplies.
<b>Interface IP change</b> (fnTrapIpChange)	The IP address for an interface has changed. The trap message includes the name of the interface, the new IP address and the serial number of the Fortinet unit. You can use this trap to track interface IP address changes for interfaces with dynamic IP addresses set using DHCP or PPPoE.

### Fortinet & FortiAnalyzer MIB fields

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

System MIB fields:

MIB field	Description
<b>fnSysSerial</b>	Fortinet unit serial number.

Administrator accounts:

MIB field	Description
<b>fnAdminNumber</b>	The number of administrators on the Fortinet unit.



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

Custom messages:

MIB field	Description
<b>fnMessages</b>	The number of custom messages on the Fortinet unit.

MIB fields and traps

MIB field	Description
<b>fmModel</b>	A table of all FortiAnalyzer models.

## Mail servers

Go to *System Settings > Advanced > Mail Server* to configure SMTP mail server settings. Mail servers can be added, edited, deleted, and tested.



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.

## Configuring a syslog server

**To add a mail server:**

Select *Create New* in the toolbar to configure mail server settings.

Create New Mail Server Settings

SMTP Server Name	<input type="text"/>
Mail Server	<input type="text"/>
SMTP Server Port	<input type="text" value="25"/>
Enable Authentication	<input type="checkbox"/>
E-Mail Account	<input type="text"/>
Password	<input type="password"/>

Configure the following settings and then select *OK*:

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

#### To test a mail server:

1. Select a server, then click *Test* in the toolbar.
2. In the *Test Mail Server* dialog box, enter an email address to send a test email to, then click *OK*.  
If the test is successful, an email will be sent to the entered email address. If the test fails, adjust the server's settings then perform a retest.

## Syslog servers

Go to *System Settings > Advanced > Syslog Server* to configure syslog mail server settings. Syslog servers can be added, edited, deleted, and tested.



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.

## Configuring a syslog server

#### To configure a syslog server:

Select *Create New* to configure a new syslog server. Configure the following settings and then select *OK*:

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

#### To test a syslog server:

Select a server, then click *Test* in the toolbar. A test log will be sent to the server. If the test fails, adjust the server's settings then perform a retest.

## Meta fields

Meta fields 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.

## Managing metadata fields

You can create, edit, and delete metadata fields from the *System Settings > Advanced > Meta Fields* page. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a meta field to display the menu.

Option	Description
Create New	Create new meta fields.
Edit	Edit the selected meta field.
Delete	Delete the selected meta field.

	Length	Importance	Status
<b>▼ Devices(6)</b>			
<input type="checkbox"/> City	50	Optional	Enabled
<input type="checkbox"/> Company/Organization	50	Optional	Enabled
<input type="checkbox"/> Contact	50	Optional	Enabled
<input type="checkbox"/> Country	50	Optional	Enabled
<input type="checkbox"/> Pelorat	20	Optional	Enabled
<input type="checkbox"/> Province/State	50	Optional	Enabled
<b>▼ Device Groups(2)</b>			
<input type="checkbox"/> Aurora	50	Required	Enabled
<input type="checkbox"/> Far Star	255	Optional	Enabled
<b>▼ Administrative Domain(3)</b>			
<input type="checkbox"/> Gaia	255	Required	Enabled
<input type="checkbox"/> Terminus	50	Required	Enabled
<input type="checkbox"/> Trantor	20	Required	Disabled

## Creating new meta fields

**To create a new meta field:**

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

<b>Object</b>	The system object to which this metadata field applies. Select either <i>Devices</i> , <i>Device Groups</i> , or <i>Administrative Domains</i> .
<b>Name</b>	Enter the label to use for the field.

<b>Length</b>	Select the maximum number of characters allowed for the field from the drop-down list: <i>20</i> , <i>50</i> , or <i>255</i> .
<b>Importance</b>	Select <i>Required</i> to make the field compulsory, otherwise select <i>Optional</i> .
<b>Status</b>	Select <i>Disabled</i> to disable this field. The default selection is <i>Enabled</i> .

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

## WSDL files

You can download Web Services Definition Language (WSDL) files.

Web services is a standards-based, platform independent, access method for other hardware and software application programming interfaces (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 GUI or CLI.

### Downloading WSDL files

To download WSDL files:

1. Go to the *System Settings > Advanced > Advanced Settings*.
2. Select the required WSDL functions.  
When you select *Legacy Operations*, no other options can be selected.
3. Click the *Download* button to download the WSDL file to your management computer.

## System configuration backups

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 create a backup after making any changes to the FortiAnalyzer configuration or to settings that affect the log devices.

### Backing up the system configuration

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

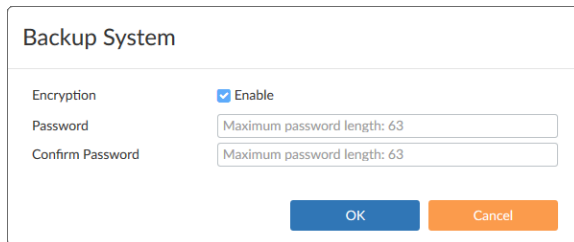


This operation does not back up log files.

---

**To back up the FortiAnalyzer configuration:**

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, find the *System Configuration* field and click *Backup*. The *Backup* dialog box opens.



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

## Restoring the system 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, find the *System Configuration* field then select *Restore*. The *Restore* dialog box appears. The *Restore* dialog box appears.
3. Configure the following settings:

<b>Choose Backup File</b>	Select <i>Browse...</i> to find the configuration backup file you want to restore on your management computer.
<b>Password</b>	Enter the encryption password, if applicable.
<b>Overwrite current IP, routing HA settings</b>	Select the check box if you need to overwrite the current IP and routing settings.

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

## Appendix A - 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 FortiGuard Distribution Network (FDN).

Traffic varies by enabled options and configured ports. Only default ports are listed.

Functionality	Port(s)
DNS lookup	UDP 53
FDN connection	TCP 443
NTP synchronization	UDP 123
SNMP traps	UDP 162
Syslog, log forwarding	UDP 514 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

**FortiAnalyzer listening ports**

Functionality	Port(s)
Syslog, log forwarding	UDP 514 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 GUI	TCP 80
HTTPS administrative access to the GUI; 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
HTTP or HTTPS administrative access to the GUI's CLI dashboard widget. Protocol used will match the protocol used by the administrator when logging in to the GUI.	TCP 2032
Log aggregation server Log aggregation server support requires model FortiAnalyzer 800 series or greater.	TCP 3000
Web Service	TCP 8080
Ping	ICMP protocol

## Appendix B - Maximum Values Matrix

The following table lists maximum values per FortiAnalyzer model.

Feature	200D	300D	1000D, 2000B	3000D, 4000B	3000E, 3500E, 3900E	VM- BASE	VM- GB1	VM- GB5	VM- GB25	VM- GB100
Administrative Domains (ADOMS)	100, 150	200	2000	2000	4000	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	200	2000	2000	256	10000	10000	10000	10000	10000
Devices/VDOMS	100, 150	200	2000	2000	4000	10000	10000	10000	10000	10000
Report output profiles	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000
SQL report templates	2000	2000	2000	2000	2000	2000	2000	2000	2000	2000



Feature	200D	300D	1000D, 2000B	3000D, 4000B	3000E, 3500E, 3900E	VM- BASE	VM- GB1	VM- GB5	VM- GB25	VM- GB100
SQL report charts	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
SQL report data-sets	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
SQL database size (GB)	No limitation for maximum database size. The size depends on the hard drive.									

## Appendix C - SNMP MIB Support

The FortiAnalyzer SNMP agent supports the following MIBs:

MIB or RFC	Description
FORTINET-CORE-MIB	This Fortinet-proprietary MIB enables your SNMP manager to query for system information and to receive traps that are common to multiple Fortinet devices.
FORTINET-FORTIMANAGER-FORTIANALYZER-MIB	This Fortinet-proprietary MIB enables your SNMP manager to query for 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.

### SNMP MIB Files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib* MIB file in the firmware image file folder. The *FORTINET-CORE-MIB.mib* file is located in the main FortiAnalyzer 5.00 file folder.

### FORTINET-CORE-MIB

```
--  
-- FORTINET-CORE-MIB.mib: Main MIB for Fortinet enterprise OID tree  
--  
-- MODULE-IDENTITY
```

```

-- OrgName
--   Fortinet Technologies, Inc.
-- ContactInfo
--   Technical Support
--   e-mail: support@fortinet.com
--   http://www.fortinet.com
--

FORTINET-CORE-MIB DEFINITIONS ::= BEGIN

IMPORTS
    ifIndex
        FROM IF-MIB
    InetAddress, InetAddressPrefixLength, InetAddressType
        FROM INET-ADDRESS-MIB
    MODULE-COMPLIANCE, NOTIFICATION-GROUP, OBJECT-GROUP
        FROM SNMPv2-CONF
    sysName
        FROM SNMPv2-MIB
    Integer32, MODULE-IDENTITY, NOTIFICATION-TYPE, OBJECT-TYPE,
    enterprises
        FROM SNMPv2-SMI
    DisplayString, TEXTUAL-CONVENTION
        FROM SNMPv2-TC;

fortinet MODULE-IDENTITY
    LAST-UPDATED "201205090000Z"
    ORGANIZATION
        "Fortinet Technologies, Inc."
    CONTACT-INFO
        "Technical Support
        email: support@fortinet.com
        http://www.fortinet.com
        "
    DESCRIPTION
        "Added fan failure and AMC bypass traps"
    REVISION "201205090000Z"
    DESCRIPTION
        "Registered FortiDDoS Mib OID"
    REVISION "201204230000Z"
    DESCRIPTION
        "Registered FortiDNS Mib OID"
    REVISION "201112230000Z"
    DESCRIPTION
        "Registered FortiCache Mib OID"
    REVISION "201104250000Z"
    DESCRIPTION
        "Supporting portuguese language"
    REVISION "201005140000Z"
    DESCRIPTION
        "Registered FortiScan Mib OID"

```

```

REVISION      "200905200000Z"
DESCRIPTION
    "MIB module for Fortinet network devices."
REVISION      "200811190000Z"
DESCRIPTION
    "Registered FortiWebMib OID"
REVISION      "200810210000Z"
DESCRIPTION
    "Added SMI comments"
REVISION      "200806250000Z"
DESCRIPTION
    "Adjusted fnAdmin tree to start at .1"
REVISION      "200806160000Z"
DESCRIPTION
    "Spelling corrections."
REVISION      "200804170000Z"
DESCRIPTION
    "Initial version of fortinet core MIB."
::= { enterprises 12356 } -- assigned by IANA

--
-- Fortinet MIB Textual Conventions (TC)
--

FnBoolState ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Boolean data type representing enabled/disabled"
    SYNTAX      INTEGER {
        disabled (1),
        enabled  (2)
    }

FnLanguage ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Enumerated type for user interface languages"
    SYNTAX      INTEGER {
        english (1),
        simplifiedChinese (2),
        japanese (3),
        korean (4),
        spanish (5),
        traditionalChinese (6),
        french (7),
        portuguese (8),
        undefined (255)
    }

FnIndex ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"

```

```

        STATUS          current
        DESCRIPTION
            "Data type for table index values"
        SYNTAX           Integer32 (0..2147483647)

FnSessionProto ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "Data type for session protocols"
    SYNTAX          INTEGER {
        ip (0),
        icmp (1),
        igmp (2),
        ipip (4),
        tcp (6),
        egp (8),
        pup (12),
        udp (17),
        idp (22),
        ipv6 (41),
        rsvp (46),
        gre (47),
        esp (50),
        ah (51),
        ospf (89),
        pim (103),
        comp (108),
        raw (255)
    }

--
-- Fortinet Enterprise Structure of Management Information (SMI)
--

fnCoreMib OBJECT IDENTIFIER ::= { fortinet 100 }

--
-- Fortinet Product Family MIB Object Identifier Assignments
--
-- fnFortiGateMib      OBJECT IDENTIFIER ::= { fortinet 101 }
-- fnFortiAnalyzerMib  OBJECT IDENTIFIER ::= { fortinet 102 }
-- fnFortiManagerMib   OBJECT IDENTIFIER ::= { fortinet 103 }
-- fnFortiDefenderMib  OBJECT IDENTIFIER ::= { fortinet 104 }
-- fnFortiMailMib      OBJECT IDENTIFIER ::= { fortinet 105 }
-- fnFortiSwitchMib    OBJECT IDENTIFIER ::= { fortinet 106 }
-- fnFortiWebMib       OBJECT IDENTIFIER ::= { fortinet 107 }
-- fnFortiScanMib      OBJECT IDENTIFIER ::= { fortinet 108 }
-- fnFortiCacheMib     OBJECT IDENTIFIER ::= { fortinet 109 }
-- fnFortiDNISMib      OBJECT IDENTIFIER ::= { fortinet 110 }
-- fnFortiDDoSMBib     OBJECT IDENTIFIER ::= { fortinet 111 }
--

```

```
--
-- fnCoreMib.fnCommon
--
fnCommon OBJECT IDENTIFIER ::= { fnCoreMib 1 }

--
-- fnCoreMib.fnCommon.fnSystem
--
fnSystem OBJECT IDENTIFIER ::= { fnCommon 1 }

fnSysSerial OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Device serial number. This is the same serial number as given
        in the ENTITY-MIB tables for the base entity."
    ::= { fnSystem 1 }

--
-- fnCoreMib.fnCommon.fnMgmt
--
fnMgmt OBJECT IDENTIFIER ::= { fnCommon 2 }

fnMgmtLanguage OBJECT-TYPE
    SYNTAX      FnLanguage
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Language used for administration interfaces"
    ::= { fnMgmt 1 }

fnAdmin OBJECT IDENTIFIER ::= { fnMgmt 100 }

fnAdminNumber OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The number of admin accounts in fnAdminTable"
    ::= { fnAdmin 1 }

fnAdminTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FnAdminEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "A table of administrator accounts on the device. This table is
        intended to be extended with platform specific information."
    ::= { fnAdmin 2 }

fnAdminEntry OBJECT-TYPE
```

```

SYNTAX      FnAdminEntry
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "An entry containing information applicable to a particular admin account"
INDEX       { fnAdminIndex }
 ::= { fnAdminTable 1 }

FnAdminEntry ::= SEQUENCE {
    fnAdminIndex      Integer32,
    fnAdminName       DisplayString,
    fnAdminAddrType   InetAddressType,
    fnAdminAddr       InetAddress,
    fnAdminMask       InetAddressPrefixLength
}

fnAdminIndex OBJECT-TYPE
    SYNTAX      Integer32 (1..2147483647)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An index uniquely defining an administrator account within the fnAd-
minTable"
    ::= { fnAdminEntry 1 }

fnAdminName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The user-name of the specified administrator account"
    ::= { fnAdminEntry 2 }

fnAdminAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The type of address stored in fnAdminAddr, in compliance with INET-
ADDRESS-MIB"
    ::= { fnAdminEntry 3 }

fnAdminAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The address prefix identifying where the administrator account can
be used from, typically an IPv4 address. The address type/format is
determined by fnAdminAddrType."
    ::= { fnAdminEntry 4 }

```

```

fnAdminMask OBJECT-TYPE
    SYNTAX      InetAddressPrefixLength
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The address prefix length (or network mask) applied to the fgAdminAddr
        to determine the subnet or host the administrator can access the device
        from"
    ::= { fnAdminEntry 5 }

--
-- fnCoreMib.fnCommon.fnTraps
--
fnTraps OBJECT IDENTIFIER ::= { fnCommon 3 }

fnTrapsPrefix OBJECT IDENTIFIER ::= { fnTraps 0 }

fnTrapObjects OBJECT IDENTIFIER ::= { fnTraps 1 }

fnGenTrapMsg OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Generic message associated with an event. The content will
        depend on the nature of the trap."
    ::= { fnTrapObjects 1 }

fnTrapCpuThreshold NOTIFICATION-TYPE
    OBJECTS      { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Indicates that the CPU usage has exceeded the configured threshold."
    ::= { fnTrapsPrefix 101 }

fnTrapMemThreshold NOTIFICATION-TYPE
    OBJECTS      { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Indicates memory usage has exceeded the configured threshold."
    ::= { fnTrapsPrefix 102 }

fnTrapLogDiskThreshold NOTIFICATION-TYPE
    OBJECTS      { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "Log disk usage has exceeded the configured threshold. Only available
        on devices with log disks."
    ::= { fnTrapsPrefix 103 }

fnTrapTempHigh NOTIFICATION-TYPE
    OBJECTS      { fnSysSerial, sysName }

```



```
STATUS      current
DESCRIPTION
    "A temperature sensor on the device has exceeded its threshold.
    Not all devices have thermal sensors. See manual for specifications."
 ::= { fnTrapsPrefix 104 }

fnTrapVoltageOutOfRange NOTIFICATION-TYPE
OBJECTS      { fnSysSerial, sysName }
STATUS      current
DESCRIPTION
    "Power levels have fluctuated outside of normal levels. Not all devices
    have voltage monitoring instrumentation. See manual for specifications."
 ::= { fnTrapsPrefix 105 }

fnTrapPowerSupplyFailure NOTIFICATION-TYPE
OBJECTS      { fnSysSerial, sysName }
STATUS      current
DESCRIPTION
    "Power supply failure detected. Not available on all models. Available
    on some devices which support redundant power supplies. See manual
    for specifications."
 ::= { fnTrapsPrefix 106 }

fnTrapAmcIfBypassMode NOTIFICATION-TYPE
OBJECTS      { fnSysSerial, sysName }
STATUS      current
DESCRIPTION
    "An AMC interface entered bypass mode. Available on models with an AMC
    expansion slot. Used with the ASM-CX4 and ASM-FX2 cards."
 ::= { fnTrapsPrefix 107 }

fnTrapFanFailure NOTIFICATION-TYPE
OBJECTS      { fnSysSerial, sysName }
STATUS      current
DESCRIPTION
    "A fan failure has been detected. Not all devices have fan sensors.
    See manual for specifications."
 ::= { fnTrapsPrefix 108 }

fnTrapIpChange NOTIFICATION-TYPE
OBJECTS      { fnSysSerial, sysName, ifIndex }
STATUS      current
DESCRIPTION
    "Indicates that the IP address of the specified interface has been
    changed."
 ::= { fnTrapsPrefix 201 }

fnTrapTest NOTIFICATION-TYPE
OBJECTS      { fnSysSerial, sysName }
STATUS      current
DESCRIPTION
    "Trap sent for diagnostic purposes by an administrator."
```

```

 ::= { fnTrapsPrefix 999 }

--
-- fnCoreMib.fnCommon.fnMIBConformance
--
fnMIBConformance OBJECT IDENTIFIER ::= { fnCoreMib 10 }

fnSystemComplianceGroup OBJECT-GROUP
    OBJECTS      { fnSysSerial }
    STATUS       current
    DESCRIPTION
        "Objects relating to the physical device."
    ::= { fnMIBConformance 1 }

fnMgmtComplianceGroup OBJECT-GROUP
    OBJECTS      { fnMgmtLanguage }
    STATUS       current
    DESCRIPTION
        "Objects relating the management of a device."
    ::= { fnMIBConformance 2 }

fnAdminComplianceGroup OBJECT-GROUP
    OBJECTS      { fnAdminNumber, fnAdminName, fnAdminAddrType,
                  fnAdminAddr, fnAdminMask }
    STATUS       current
    DESCRIPTION
        "Administration access control objects."
    ::= { fnMIBConformance 3 }

fnTrapsComplianceGroup NOTIFICATION-GROUP
    NOTIFICATIONS { fnTrapCpuThreshold, fnTrapMemThreshold,
                  fnTrapLogDiskThreshold, fnTrapTempHigh,
                  fnTrapVoltageOutOfRange, fnTrapPowerSupplyFailure,
                  fnTrapAmcIfBypassMode, fnTrapFanFailure,
                  fnTrapIpChange, fnTrapTest }
    STATUS       current
    DESCRIPTION
        "Event notifications"
    ::= { fnMIBConformance 4 }

fnNotifObjectsComplianceGroup OBJECT-GROUP
    OBJECTS      { fnGenTrapMsg }
    STATUS       current
    DESCRIPTION
        "Object identifiers used in notifications"
    ::= { fnMIBConformance 5 }

fnMIBCompliance MODULE-COMPLIANCE
    STATUS       current
    DESCRIPTION
        "The compliance statement for the application MIB."

```

```

MODULE      -- this module

GROUP      fnSystemComplianceGroup
DESCRIPTION
    "This group is mandatory for all Fortinet network appliances
    supporting this MIB."

GROUP      fnMgmtComplianceGroup
DESCRIPTION
    "This group is optional for devices that do not support common
    management interface options such as multiple languages."

GROUP      fnAdminComplianceGroup
DESCRIPTION
    "This group should be accessible on any device supporting
    administrator authentication."

GROUP      fnTrapsComplianceGroup
DESCRIPTION
    "Traps are optional. Not all models support all traps. Consult
    product literature to see which traps are supported."

GROUP      fnNotifObjectsComplianceGroup
DESCRIPTION
    "Object identifiers used in notifications. Objects are required
    if their containing trap is implemented."

 ::= { fnMIBConformance 100 }

END

```

## FORTINET-FORTIMANAGER-FORTIANALYZER-MIB

```

FORTINET-FORTIMANAGER-FORTIANALYZER-MIB DEFINITIONS ::= BEGIN

IMPORTS
    fnSysSerial, fortinet, FnIndex, FnBoolState, fnGenTrapMsg
        FROM FORTINET-CORE-MIB
    sysName
        FROM SNMPv2-MIB
    InetPortNumber
        FROM INET-ADDRESS-MIB
    MODULE-COMPLIANCE, NOTIFICATION-GROUP, OBJECT-GROUP
        FROM SNMPv2-CONF
    MODULE-IDENTITY, NOTIFICATION-TYPE, OBJECT-TYPE,
    Integer32, Gauge32, Counter32, Counter64, IPAddress
        FROM SNMPv2-SMI
    DisplayString, TEXTUAL-CONVENTION
        FROM SNMPv2-TC;

```

```

fnFortiManagerMib MODULE-IDENTITY
    LAST-UPDATED "201508150000Z"
    ORGANIZATION
        "Fortinet Technologies, Inc."
    CONTACT-INFO
        "
            Technical Support
            email: support@fortinet.com
            http://www.fortinet.com"
    DESCRIPTION
        "Add fmSysVer-
sion, fmSysUpTime, fmLogRate, fmAdom, fmDevice, fmRaid, fmPower, fmHa"
    REVISION      "201508150000Z"
    DESCRIPTION
        "Add model names faz3000E, fmg4000E, faz1000D, fmg1000D."
    REVISION      "201404220000Z"
    DESCRIPTION
        "Added fmSysCpuUsageExcludedNice.
        Added fmTrapCpuThresholdExcludeNice."
    REVISION      "201306100000Z"
    DESCRIPTION
        "Add support for FortiAnalyzer."
    REVISION      "201303270000Z"
    DESCRIPTION
        "Added license gb/day and device quota trap. fmTrapLicGbDayThreshold
        and fmTrapLicDevQuotaThreshold"
    REVISION      "201211260000Z"
    DESCRIPTION
        "Added commas between notifications in NOTIFICATION-GROUP.
        Added imports from SNMPv2-SMI and SNMPv2-TC.
        imported `OBJECT-GROUP' from module SNMPv2-CONF"
    REVISION      "201204200000Z"
    DESCRIPTION
        "Added RAID trap fmTrapRAIDStatusChange."
    REVISION      "201103250000Z"
    DESCRIPTION
        "Added fmSysMemUsed, fmSysMemCapacity, fmSysCpuUsage.
        Added new FortiManager models."
    REVISION      "201101190000Z"
    DESCRIPTION
        "MIB module for Fortinet FortiManager devices."
    REVISION      "200807180000Z"
    DESCRIPTION
        "Add sysName to fmTrapHASwitch."
    REVISION      "200806260000Z"
    DESCRIPTION
        "OID correction for fnFortiManagerMib."
    REVISION      "200806160000Z"
    DESCRIPTION
        "Spelling corrections."
    REVISION      "200806100000Z"
    DESCRIPTION

```

```

        "Initial version of FORTINET-FORTIMANAGER-MIB."
        ::= { fortinet 103 }

--
-- fortinet.fnFortiManagerMib.fmTraps
--

FmRAIDStatusCode ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "Enumerated list of RAID status codes."
    SYNTAX           INTEGER { arrayOK(1), arrayDegraded(2), arrayFailed(3),
                                arrayRebuilding(4), arrayRebuildingStarted(5),
                                arrayRebuildingFinished(6), arrayInitializing(7),
                                arrayInitializingStarted(8), arrayInitializingFinished(9),
                                diskOk(10), diskDegraded(11), diskFailEvent(12),
                                diskUnavailable(100), diskUnused(101), diskOK(102), diskRebuilding(103),
                                diskFailed(104), diskSpare(105),
                                raidUnavailable(200), raidOK(201), raidDegraded(202), raidFailed(203),
                                raidBackground-Initializing(204), raidBackground-Verifying(205), raidBackground-
                                Rebuilding(206) }

FmSessProto ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "data type for session protocols"
    SYNTAX           INTEGER { ip(0), icmp(1), igmp(2), ipip(4), tcp(6),
                                egp(8), pup(12), udp(17), idp(22), ipv6(41),
                                rsvp(46), gre(47), esp(50), ah(51), ospf(89),
                                pim(103), comp(108), raw(255) }

fmTraps OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 0 }

fmTrapPrefix OBJECT IDENTIFIER
    ::= { fmTraps 0 }

fmTrapObject OBJECT IDENTIFIER
    ::= { fmTraps 1 }

fmRAIDStatus OBJECT-TYPE
    SYNTAX          FmRAIDStatusCode
    MAX-ACCESS      accessible-for-notify
    STATUS          current
    DESCRIPTION
        "New RAID state associated with a RAID status change event."
    ::= { fmTrapObject 1 }

fmRAIDDevIndex OBJECT-TYPE
    SYNTAX          DisplayString (SIZE(0..32))

```

```
MAX-ACCESS    accessible-for-notify
STATUS        current
DESCRIPTION
    "Name/index of a RAID device relating to the event."
::= { fmTrapObject 2 }
```

```
fmLogRate OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Log receiving rate in number of logs per second."
    ::= { fmTrapObject 3 }
```

```
fmLogRateThreshold OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Threshold for log rate in number of logs per second."
    ::= { fmTrapObject 4 }
```

```
fmLogDataRate OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Log receiving data rate in number of KB per second."
    ::= { fmTrapObject 5 }
```

```
fmLogDataRateThreshold OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Threshold for log data rate in number of KB per second."
    ::= { fmTrapObject 6 }
```

```
fmLicGbDay OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Log data used in number of GB per day."
    ::= { fmTrapObject 7 }
```

```
fmLicGbDayThreshold OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Licensed threshold for log data in number of GB per day."
```

```
 ::= { fmTrapObject 8 }

fmLicDevQuota OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Device quota used in number of GB."
    ::= { fmTrapObject 9 }

fmLicDevQuotaThreshold OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "Licensed threshold for device quota in number of GB."
    ::= { fmTrapObject 10 }

--
-- fortinet.fnFortiManagerMib.fmModel
--

fmModel OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 1 }

fmgl100 OBJECT IDENTIFIER
    ::= { fmModel 1000 }

fmglvm OBJECT IDENTIFIER
    ::= { fmModel 1001 }

fmgl100C OBJECT IDENTIFIER
    ::= { fmModel 1003 }

fmgl200D OBJECT IDENTIFIER
    ::= { fmModel 2004 }

fmgl300D OBJECT IDENTIFIER
    ::= { fmModel 3004 }

fmgl400 OBJECT IDENTIFIER
    ::= { fmModel 4000 }

fmgl400A OBJECT IDENTIFIER
    ::= { fmModel 4001 }

fmgl400B OBJECT IDENTIFIER
    ::= { fmModel 4002 }

fmgl400C OBJECT IDENTIFIER
    ::= { fmModel 4003 }
```

```
fmg1000C OBJECT IDENTIFIER
 ::= { fmModel 10003 }

fmg1000D OBJECT IDENTIFIER
 ::= { fmModel 10004 }

fmg2000XL OBJECT IDENTIFIER
 ::= { fmModel 20000 }

fmg3000 OBJECT IDENTIFIER
 ::= { fmModel 30000 }

fmg3000B OBJECT IDENTIFIER
 ::= { fmModel 30002 }

fmg3000C OBJECT IDENTIFIER
 ::= { fmModel 30003 }

fmg3900E OBJECT IDENTIFIER
 ::= { fmModel 39005 }

fmg4000D OBJECT IDENTIFIER
 ::= { fmModel 40004 }

fmg4000E OBJECT IDENTIFIER
 ::= { fmModel 40005 }

fmg5001A OBJECT IDENTIFIER
 ::= { fmModel 50011 }

--
-- fortinet.fnFortiManagerMib.fmSystem
--

fmSystem OBJECT IDENTIFIER
 ::= { fnFortiManagerMib 2 }

--
-- fortinet.fnFortiManagerMib.fmSystem.fmSystemInfo
--

fmSystemInfo OBJECT IDENTIFIER
 ::= { fmSystem 1 }

fmSysCpuUsage OBJECT-TYPE
    SYNTAX      Integer32 (0..100)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Current CPU usage (percentage)"
    ::= { fmSystemInfo 1 }
```



```
fmSysMemUsed OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Current memory used (KB) "
    ::= { fmSystemInfo 2 }

fmSysMemCapacity OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Total physical and swap memory installed (KB) "
    ::= { fmSystemInfo 3 }

fmSysDiskUsage OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Current hard disk usage (MB) "
    ::= { fmSystemInfo 4 }

fmSysDiskCapacity OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Total hard disk capacity (MB) "
    ::= { fmSystemInfo 5 }

fmSysCpuUsageExcludedNice OBJECT-TYPE
    SYNTAX      Gauge32 (0..100)
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Current CPU usage excluded nice processes usage (percentage) "
    ::= { fmSystemInfo 6 }

fmSysVersion OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Firmware version of the device"
    ::= { fmSystemInfo 7 }

fmSysUpTime OBJECT-TYPE
    SYNTAX      Counter64
    UNITS        "hundredths of a second"
    MAX-ACCESS   read-only
```

```

        STATUS      current
        DESCRIPTION
            "The 64bit time (in hundredths of a second) since the network management
            portion of the system was last re-initialized."
        ::= { fmSystemInfo 8 }

fmLogRate OBJECT-TYPE
    SYNTAX      Gauge32
    UNITS        "logs per second"
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Log receiving rate in number of logs per second."
    ::= { fmSystemInfo 9 }

fmTrapHASwitch NOTIFICATION-TYPE
    OBJECTS      { fnSysSerial, sysName }
    STATUS      current
    DESCRIPTION
        "FortiManager HA cluster has been re-arranged. A new master has been selected
        and asserted."
    ::= { fmTrapPrefix 401 }

fmTrapRAIDStatusChange NOTIFICATION-TYPE
    OBJECTS      { fnSysSerial, sysName,
                    fmRAIDStatus, fmRAIDDevIndex }
    STATUS      current
    DESCRIPTION
        "Trap is sent when there is a change in the status of the RAID array, if
        present."
    ::= { fmTrapPrefix 402 }

fmTrapLogAlert NOTIFICATION-TYPE
    OBJECTS      { fnSysSerial, sysName, fnGenTrapMsg }
    STATUS      current
    DESCRIPTION
        "Trap is sent when a log based alert has been triggered.
        Alert description included in trap."
    ::= { fmTrapPrefix 403 }

fmTrapLogRateThreshold NOTIFICATION-TYPE
    OBJECTS      { fnSysSerial, sysName, fmLogRate, fmLogRateThreshold }
    STATUS      current
    DESCRIPTION
        "Indicates that the incoming log rate has exceeded the threshold"
    ::= { fmTrapPrefix 404 }

fmTrapLogDataRateThreshold NOTIFICATION-TYPE
    OBJECTS      { fnSysSerial, sysName, fmLogDataRate, fmLogDataRateThreshold }
    STATUS      current
    DESCRIPTION
        "Indicates that the incoming log data rate has exceeded the threshold"

```

```
 ::= { fmTrapPrefix 405 }

fmTrapLicGbDayThreshold NOTIFICATION-TYPE
    OBJECTS      { fnSysSerial, sysName, fmLicGbDay, fmLicGbDayThreshold }
    STATUS       current
    DESCRIPTION   "Indicates that the used log has exceeded the licensed GB/Day"
    ::= { fmTrapPrefix 407 }

fmTrapLicDevQuotaThreshold NOTIFICATION-TYPE
    OBJECTS      { fnSysSerial, sysName, fmLicDevQuota, fmLicDevQuotaThreshold }
    STATUS       current
    DESCRIPTION   "Indicates that the used device quota has exceeded the licensed device
quota"
    ::= { fmTrapPrefix 408 }

fmTrapCpuThresholdExcludeNice NOTIFICATION-TYPE
    OBJECTS      { fnSysSerial, sysName }
    STATUS       current
    DESCRIPTION   "Indicates that the CPU usage excluding nice processes has exceeded the
threshold"
    ::= { fmTrapPrefix 409 }

--
-- fortinet.fnFortiManagerMib.faModel
--

faModel OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 3 }

faz100 OBJECT IDENTIFIER
    ::= { faModel 1000 }

faz100A OBJECT IDENTIFIER
    ::= { faModel 1001 }

faz100B OBJECT IDENTIFIER
    ::= { faModel 1002 }

faz100C OBJECT IDENTIFIER
    ::= { faModel 1003 }

faz200D OBJECT IDENTIFIER
    ::= { faModel 2004 }

faz300D OBJECT IDENTIFIER
    ::= { faModel 3004 }

faz400 OBJECT IDENTIFIER
    ::= { faModel 4000 }
```

```
faz400B OBJECT IDENTIFIER
::= { faModel 4002 }

faz400C OBJECT IDENTIFIER
::= { faModel 4003 }

fazvm OBJECT IDENTIFIER
::= { faModel 20 }

faz800 OBJECT IDENTIFIER
::= { faModel 8000 }

faz800B OBJECT IDENTIFIER
::= { faModel 8002 }

faz1000B OBJECT IDENTIFIER
::= { faModel 10002 }

faz1000C OBJECT IDENTIFIER
::= { faModel 10003 }

faz1000D OBJECT IDENTIFIER
::= { faModel 10004 }

faz2000 OBJECT IDENTIFIER
::= { faModel 20000 }

faz2000A OBJECT IDENTIFIER
::= { faModel 20001 }

faz2000B OBJECT IDENTIFIER
::= { faModel 20002 }

faz3000D OBJECT IDENTIFIER
::= { faModel 30004 }

faz3000E OBJECT IDENTIFIER
::= { faModel 30005 }

faz3500E OBJECT IDENTIFIER
::= { faModel 35005 }

faz3900E OBJECT IDENTIFIER
::= { faModel 39005 }

faz4000 OBJECT IDENTIFIER
::= { faModel 40000 }

faz4000A OBJECT IDENTIFIER
::= { faModel 40001 }
```

```

faz4000B OBJECT IDENTIFIER
    ::= { faModel 40002 }

--
-- fortinet.fnFortiManagerMib.fmInetProto
--

fmInetProto OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 4 }

fmInetProtoInfo OBJECT IDENTIFIER
    ::= { fmInetProto 1 }

fmInetProtoTables OBJECT IDENTIFIER
    ::= { fmInetProto 2 }

fmIpSessTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FmIpSessEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Information on the IP sessions active on the device"
    ::= { fmInetProtoTables 1 }

fmIpSessEntry OBJECT-TYPE
    SYNTAX      FmIpSessEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Information on a specific session, including source and destination"
    INDEX       { fmIpSessIndex }
    ::= { fmIpSessTable 1 }

FmIpSessEntry ::= SEQUENCE {
    fmIpSessIndex      FnIndex,
    fmIpSessProto      FmSessProto,
    fmIpSessFromAddr   IpAddress,
    fmIpSessFromPort   InetPortNumber,
    fmIpSessToAddr     IpAddress,
    fmIpSessToPort     InetPortNumber,
    fmIpSessExp        Counter32
}

fmIpSessIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An index value that uniquely identifies
         an IP session within the fmIpSessTable"
    ::= { fmIpSessEntry 1 }

```

```
fmIpSessProto OBJECT-TYPE
    SYNTAX      FmSessProto
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The protocol the session is using (IP, TCP, UDP, etc.)"
    ::= { fmIpSessEntry 2 }

fmIpSessFromAddr OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Source IP address (IPv4 only) of the session"
    ::= { fmIpSessEntry 3 }

fmIpSessFromPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Source port number (UDP and TCP only) of the session"
    ::= { fmIpSessEntry 4 }

fmIpSessToAddr OBJECT-TYPE
    SYNTAX      IpAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Destination IP address (IPv4 only) of the session"
    ::= { fmIpSessEntry 5 }

fmIpSessToPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Destination Port number (UDP and TCP only) of the session"
    ::= { fmIpSessEntry 6 }

fmIpSessExp OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of seconds remaining before the session expires (if idle)"
    ::= { fmIpSessEntry 7 }

--
-- fortinet.fnFortiManagerMib.fmAdom
--
```

```

fmAdom OBJECT IDENTIFIER
 ::= { fnFortiManagerMib 5 }

fmAdomInfo OBJECT IDENTIFIER
 ::= { fmAdom 1 }

fmAdomEnabled OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Whether administrative domains are enabled on this device"
    ::= { fmAdomInfo 1 }

fmAdomNumber OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The number of administrative domains in fmAdomTable"
    ::= { fmAdomInfo 2 }

fmAdomMax OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The maximum number of administrative domains allowed on the device as
        allowed by hardware and/or licensing"
    ::= { fmAdomInfo 3 }

fmAdomTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FmAdomEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "A table of administrative domains configured on the device"
    ::= { fmAdom 2 }

fmAdomEntry OBJECT-TYPE
    SYNTAX      FmAdomEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "An entry containing information applicable
        to a particular administrative domain"
    INDEX       { fmAdomEntIndex }
    ::= { fmAdomTable 1 }

FmAdomEntry ::= SEQUENCE {
    fmAdomEntIndex      FnIndex,
    fmAdomEntName       DisplayString,

```

```

    fmAdomEntState      FnBoolState,
    fmAdomEntMode       FmAdomEntMode,
    fmAdomEntFgtNumber  Integer32,
    fmAdomEntPolicyPackageNumber Integer32,
    fmAdomEntOsVersion  Integer32,
    fmAdomEntMr         Integer32,
    fmAdomEntVpnMode    FmAdomEntVpnMode
}

fmAdomEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An index value that uniquely identifies the entry"
    ::= { fmAdomEntry 1 }

fmAdomEntName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The name of the administrative domain"
    ::= { fmAdomEntry 2 }

fmAdomEntState OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Whether adom is enabled or disabled"
    ::= { fmAdomEntry 3 }

FmAdomEntMode ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Whether adom is in normal or backup mode"
    SYNTAX      INTEGER {
        normal (1),
        backup (2)
    }

fmAdomEntMode OBJECT-TYPE
    SYNTAX      FmAdomEntMode
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Whether adom is in normal or backup mode"
    ::= { fmAdomEntry 4 }

fmAdomEntFgtNumber OBJECT-TYPE
    SYNTAX      Integer32

```



```

MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
    "Number of FortiGates in adom"
 ::= { fmAdomEntry 5 }

fmAdomEntPolicyPackageNumber OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Number of policy packages in adom"
    ::= { fmAdomEntry 6 }

fmAdomEntOsVersion OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "OS version supported by adom"
    ::= { fmAdomEntry 7 }

fmAdomEntMr OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "MR version supported by adom"
    ::= { fmAdomEntry 8 }

FmAdomEntVpnMode ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Adom VPN mode"
    SYNTAX      INTEGER {
        central-console (1),
        policy-and-device (2),
        not-applicable (3)
    }

fmAdomEntVpnMode OBJECT-TYPE
    SYNTAX      FmAdomEntVpnMode
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Adom VPN mode"
    ::= { fmAdomEntry 9 }

--
-- fortinet.fnFortiManagerMib.fmDevice
--

```

```

fmDevice OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 6 }

fmDeviceInfo OBJECT IDENTIFIER
    ::= { fmDevice 1 }

fmDeviceNumber OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The number of devices in fmDeviceTable"
    ::= { fmDeviceInfo 1 }

fmDeviceTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FmDeviceEntry
    MAX-ACCESS   not-accessible
    STATUS      current
    DESCRIPTION
        "A table of devices configured on the device"
    ::= { fmDevice 2 }

fmDeviceEntry OBJECT-TYPE
    SYNTAX      FmDeviceEntry
    MAX-ACCESS   not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable
         to a particular device"
    INDEX       { fmDeviceEntIndex }
    ::= { fmDeviceTable 1 }

FmDeviceEntry ::= SEQUENCE {
    fmDeviceEntIndex      FnIndex,
    fmDeviceEntName       DisplayString,
    fmDeviceEntSn         DisplayString,
    fmDeviceEntMode       FmDeviceEntMode,
    fmDeviceEntAdom       DisplayString,
    fmDeviceEntIp         DisplayString,
    fmDeviceEntOsVersion  Integer32,
    fmDeviceEntMr         Integer32,
    fmDeviceEntBuild      Integer32,
    fmDeviceEntHaMode     FmDeviceEntHaMode,
    fmDeviceEntHaGroup    DisplayString,
    fmDeviceEntConnectState FmDeviceEntConnectState,
    fmDeviceEntDbState    FmDeviceEntDbState,
    fmDeviceEntConfigState FmDeviceEntConfigState,
    fmDeviceEntState      FmDeviceEntState,
    fmDeviceEntPlatform   DisplayString,
    fmDeviceEntVdomEnabled FnBoolState,
    fmDeviceEntSupportState FmDeviceEntSupportState,
    fmDeviceEntAvExpireDate DisplayString,

```

```

    fmDeviceEntIpsExpireDate DisplayString,
    fmDeviceEntWfExpireDate DisplayString,
    fmDeviceEntAsExpireDate DisplayString,
    fmDeviceEntPolicyPackageState FmDeviceEntPolicyPackageState,
    fmDeviceEntDesc          DisplayString
}

fmDeviceEntIndex OBJECT-TYPE
    SYNTAX          FnIndex
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "An index value that uniquely identifies the entry"
    ::= { fmDeviceEntry 1 }

fmDeviceEntName OBJECT-TYPE
    SYNTAX          DisplayString
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The name of the device"
    ::= { fmDeviceEntry 2 }

fmDeviceEntSn OBJECT-TYPE
    SYNTAX          DisplayString
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The serial number of the device"
    ::= { fmDeviceEntry 3 }

FmDeviceEntMode ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "Device management mode"
    SYNTAX          INTEGER {
        unregistered (0),
        fmg (1),
        faz (2),
        fmg-faz (3)
    }

fmDeviceEntMode OBJECT-TYPE
    SYNTAX          FmDeviceEntMode
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "Device management mode"
    ::= { fmDeviceEntry 4 }

fmDeviceEntAdom OBJECT-TYPE
    SYNTAX          DisplayString

```

```

MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
    "The adom name the device belongs to"
::= { fmDeviceEntry 5 }

fmDeviceEntIp OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The IP of the device"
    ::= { fmDeviceEntry 6 }

fmDeviceEntOsVersion OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The OS version of the device"
    ::= { fmDeviceEntry 7 }

fmDeviceEntMr OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The MR version of the device"
    ::= { fmDeviceEntry 8 }

fmDeviceEntBuild OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The build number of the device"
    ::= { fmDeviceEntry 9 }

FmDeviceEntHaMode ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Device HA mode"
    SYNTAX      INTEGER {
        standalone (0),
        a-p (1),
        a-a (2),
        elbc (3),
        dual (4),
        fmg (5)
    }

fmDeviceEntHaMode OBJECT-TYPE

```

```
SYNTAX      FmDeviceEntHaMode
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "Device HA mode"
 ::= { fmDeviceEntry 10 }

fmDeviceEntHaGroup OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Device HA group name"
    ::= { fmDeviceEntry 11 }

FmDeviceEntConnectState ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Device connection status"
    SYNTAX      INTEGER {
        unknown (0),
        up (1),
        down (2)
    }

fmDeviceEntConnectState OBJECT-TYPE
    SYNTAX      FmDeviceEntConnectState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Device connection status"
    ::= { fmDeviceEntry 12 }

FmDeviceEntDbState ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Device DB status"
    SYNTAX      INTEGER {
        unknown (0),
        not-modified (1),
        modified (2)
    }

fmDeviceEntDbState OBJECT-TYPE
    SYNTAX      FmDeviceEntDbState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Device DB status"
    ::= { fmDeviceEntry 13 }

FmDeviceEntConfigState ::= TEXTUAL-CONVENTION
```

```

STATUS      current
DESCRIPTION
    "Device config status"
SYNTAX      INTEGER {
    unknown (0),
    in-sync (1),
    out-of-sync (2)
}

fmDeviceEntConfigState OBJECT-TYPE
    SYNTAX      FmDeviceEntConfigState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Device config status"
    ::= { fmDeviceEntry 14 }

FmDeviceEntState ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Device status"
    SYNTAX      INTEGER {
        none (0),
        unknown (1),
        checked-in (2),
        in-progress (3),
        installed (4),
        aborted (5),
        sched (6),
        retry (7),
        canceled (8),
        pending (9),
        retrieved (10),
        changed-conf (11),
        sync-fail (12),
        timeout (13),
        rev-reverted (14),
        auto-updated (15)
    }

fmDeviceEntState OBJECT-TYPE
    SYNTAX      FmDeviceEntState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Device status"
    ::= { fmDeviceEntry 15 }

fmDeviceEntPlatform OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-only
    STATUS      current

```

```
DESCRIPTION
    "The platform of the device"
 ::= { fmDeviceEntry 16 }

fmDeviceEntVdomEnabled OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Whether vdom enabled on the device"
 ::= { fmDeviceEntry 17 }

FmDeviceEntSupportState ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "The support status of the device"
    SYNTAX       INTEGER {
        expired  (0),
        valid    (1)
    }

fmDeviceEntSupportState OBJECT-TYPE
    SYNTAX      FmDeviceEntSupportState
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The support status of the device"
 ::= { fmDeviceEntry 18 }

fmDeviceEntAvExpireDate OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The AV license of the device"
 ::= { fmDeviceEntry 19 }

fmDeviceEntIpsExpireDate OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The IPS license of the device"
 ::= { fmDeviceEntry 20 }

fmDeviceEntWfExpireDate OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The WCF license of the device"
 ::= { fmDeviceEntry 21 }
```

```

fmDeviceEntAsExpireDate OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The AS license of the device"
    ::= { fmDeviceEntry 22 }

FmDeviceEntPolicyPackageState ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "The policy package status of the device"
    SYNTAX       INTEGER {
        never-installed (-1),
        installed (0),
        modified (1),
        imported (2),
        unknown (3),
        out-of-sync (9),
        conflict (10)
    }

fmDeviceEntPolicyPackageState OBJECT-TYPE
    SYNTAX       FmDeviceEntPolicyPackageState
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The policy package status of the device"
    ::= { fmDeviceEntry 23 }

fmDeviceEntDesc OBJECT-TYPE
    SYNTAX       DisplayString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The description of the device"
    ::= { fmDeviceEntry 24 }

--
-- fortinet.fnFortiManagerMib.fmRaid
--

fmRaid OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 7 }

fmRaidInfo OBJECT IDENTIFIER
    ::= { fmRaid 1 }

FmRaidLevel ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION

```



```

        "Raid level"
SYNTAX      INTEGER {
    unavailable (0),
    linear      (1),
    raid-0      (2),
    raid-1      (3),
    raid-1s     (4),
    raid-5      (5),
    raid-5s     (6),
    raid-6      (7),
    raid-6s     (8),
    raid-10     (9),
    raid-10s    (10),
    raid-50     (11),
    raid-50s    (12),
    raid-60     (13),
    raid-60s    (14)
}

fmRaidLevel OBJECT-TYPE
    SYNTAX      FmRaidLevel
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Raid level"
    ::= { fmRaidInfo 1 }

FmRaidState ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "Raid status"
    SYNTAX      INTEGER {
        unavailable (0),
        ok (1),
        degraded (2),
        failed (3),
        background-initializing (4),
        background-verifying (5),
        background-rebuilding (6)
    }

fmRaidState OBJECT-TYPE
    SYNTAX      FmRaidState
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Raid status"
    ::= { fmRaidInfo 2 }

fmRaidSize OBJECT-TYPE
    SYNTAX      Integer32
    UNITS        "GB"

```

```

MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
    "Raid size in GB"
::= { fmRaidInfo 3 }

fmRaidDiskNumber OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Disk numbers in the Raid"
    ::= { fmRaidInfo 4 }

fmRaidDiskTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FmRaidDiskEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of disks in the raid"
    ::= { fmRaid 2 }

fmRaidDiskEntry OBJECT-TYPE
    SYNTAX      FmRaidDiskEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable
         to a particular raid disk"
    INDEX       { fmRaidDiskEntIndex }
    ::= { fmRaidDiskTable 1 }

FmRaidDiskEntry ::= SEQUENCE {
    fmRaidDiskEntIndex      FnIndex,
    fmRaidDiskEntState      FmRaidDiskEntState,
    fmRaidDiskEntSize       Integer32
}

fmRaidDiskEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An index value that uniquely identifies the entry"
    ::= { fmRaidDiskEntry 1 }

FmRaidDiskEntState ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        "Raid disk status"
    SYNTAX      INTEGER {
        unavailable (0),

```

```

        unused (1),
        ok (2),
        rebuilding (3),
        failed (4),
        spare (5)
    }

fmRaidDiskEntState OBJECT-TYPE
    SYNTAX      FmRaidDiskEntState
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Raid disk status"
    ::= { fmRaidDiskEntry 2 }

fmRaidDiskEntSize OBJECT-TYPE
    SYNTAX      Integer32
    UNITS       "GB"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Raid disk size in GB"
    ::= { fmRaidDiskEntry 3 }

--
-- fortinet.fnFortiManagerMib.fmPower
--

fmPower OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 8 }

fmPowerTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FmPowerEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of power supply status"
    ::= { fmPower 2 }

fmPowerEntry OBJECT-TYPE
    SYNTAX      FmPowerEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing information applicable
         to a particular power supply unit"
    INDEX       { fmPowerEntIndex }
    ::= { fmPowerTable 1 }

FmPowerEntry ::= SEQUENCE {
    fmPowerEntIndex      FnIndex,
    fmPowerEntState      FmPowerEntState

```

```

}

fmPowerEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "An index value that uniquely identifies the entry"
    ::= { fmPowerEntry 1 }

FmPowerEntState ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "Power supply unit status"
    SYNTAX       INTEGER {
        unknown (-1),
        offline (0),
        online (1)
    }

fmPowerEntState OBJECT-TYPE
    SYNTAX       FmPowerEntState
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Power supply unit status"
    ::= { fmPowerEntry 2 }

--
-- fortinet.fnFortiManagerMib.fmHa
--

fmHa OBJECT IDENTIFIER
    ::= { fnFortiManagerMib 9 }

fmHaInfo OBJECT IDENTIFIER
    ::= { fmHa 1 }

FmHaMode ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "Ha mode"
    SYNTAX       INTEGER {
        standalone (0),
        master (1),
        slave (2)
    }

fmHaMode OBJECT-TYPE
    SYNTAX       FmHaMode
    MAX-ACCESS   read-only
    STATUS       current

```

```

DESCRIPTION
    "Ha mode"
 ::= { fmHaInfo 1 }

fmHaClusterId OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Ha cluster ID"
 ::= { fmHaInfo 2 }

fmHaPeerNumber OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Peer numbers in the Ha"
 ::= { fmHaInfo 3 }

fmHaPeerTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF FmHaPeerEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "A table of peers in the Ha"
 ::= { fmHa 2 }

fmHaPeerEntry OBJECT-TYPE
    SYNTAX      FmHaPeerEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "An entry containing information applicable
         to a particular Ha peer"
    INDEX       { fmHaPeerEntIndex }
 ::= { fmHaPeerTable 1 }

FmHaPeerEntry ::= SEQUENCE {
    fmHaPeerEntIndex      FnIndex,
    fmHaPeerEntIp         DisplayString,
    fmHaPeerEntSn         DisplayString,
    fmHaPeerEntEnabled    FnBoolState,
    fmHaPeerEntHostName   DisplayString,
    fmHaPeerEntState      FmHaPeerEntState
}

fmHaPeerEntIndex OBJECT-TYPE
    SYNTAX      FnIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION

```

```
        "An index value that uniquely identifies the entry"
 ::= { fmHaPeerEntry 1 }

fmHaPeerEntIp OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Peer IP"
    ::= { fmHaPeerEntry 2 }

fmHaPeerEntSn OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Peer serial number"
    ::= { fmHaPeerEntry 3 }

fmHaPeerEntEnabled OBJECT-TYPE
    SYNTAX      FnBoolState
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Whether peer is enabled"
    ::= { fmHaPeerEntry 4 }

fmHaPeerEntHostName OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Peer host name"
    ::= { fmHaPeerEntry 5 }

FmHaPeerEntState ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "Peer status"
    SYNTAX      INTEGER {
        down (0),
        negotiating (1),
        synchronizing (2),
        up (3)
    }

fmHaPeerEntState OBJECT-TYPE
    SYNTAX      FmHaPeerEntState
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Peer status"
```

```

 ::= { fmHaPeerEntry 6 }

--
-- fortinet.fnFortiManagerMib.fmMibConformance
--

fmMIBConformance OBJECT IDENTIFIER
 ::= { fnFortiManagerMib 10 }

fmTrapsComplianceGroup NOTIFICATION-GROUP
 NOTIFICATIONS { fmTrapHASwitch, fmTrapRAIDStatusChange,
                 fmTrapLogAlert, fmTrapLogRateThreshold,
                 fmTrapLogDataRateThreshold,
                 fmTrapLicGbDayThreshold,
                 fmTrapLicDevQuotaThreshold,
                 fmTrapCpuThresholdExcludeNice }
 STATUS      current
 DESCRIPTION
   "Event notifications"
 ::= { fmMIBConformance 1 }

fmSystemObjectGroup OBJECT-GROUP
 OBJECTS      { fmSysMemUsed, fmSysMemCapacity,
                 fmSysCpuUsage, fmSysDiskCapacity,
                 fmSysDiskUsage, fmSysCpuUsageExcludedNice }
 STATUS      current
 DESCRIPTION
   "Objects pertaining to the system status of the device."
 ::= { fmMIBConformance 2 }

fmNotificationObjComplianceGroup OBJECT-GROUP
 OBJECTS      { fmRAIDStatus, fmRAIDDevIndex,
                 fmLogRate, fmLogRateThreshold,
                 fmLogDataRate, fmLogDataRateThreshold,
                 fmLicGbDay, fmLicGbDayThreshold,
                 fmLicDevQuota, fmLicDevQuotaThreshold }
 STATUS      current
 DESCRIPTION
   "Object identifiers used in notifications"
 ::= { fmMIBConformance 3 }

fmSessionComplianceGroup OBJECT-GROUP
 OBJECTS {
   fmIpSessProto,
   fmIpSessFromAddr,
   fmIpSessFromPort,
   fmIpSessToAddr,
   fmIpSessToPort,
   fmIpSessExp
 }
 STATUS current
 DESCRIPTION "Session related instrumentation"

```

```
::= { fmMIBConformance 4 }

fmMIBCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
        "The compliance statement for the FortiManager FortiAnalyzer MIB."

    MODULE      -- this module

        GROUP    fmTrapsComplianceGroup
        DESCRIPTION
            "Traps are optional. Not all models support all traps. Consult
            product literature to see which traps are supported."

        GROUP    fmSystemObjectGroup
        DESCRIPTION
            "Model and feature specific."

        GROUP    fmNotificationObjComplianceGroup
        DESCRIPTION
            "Object identifiers used in notifications. Objects are required if
            their containing trap is implemented."

        GROUP    fmSessionComplianceGroup
        DESCRIPTION
            "IP session related implementation."

::= { fmMIBConformance 100 }

END -- end of module FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.
```





High Performance Network Security



Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.