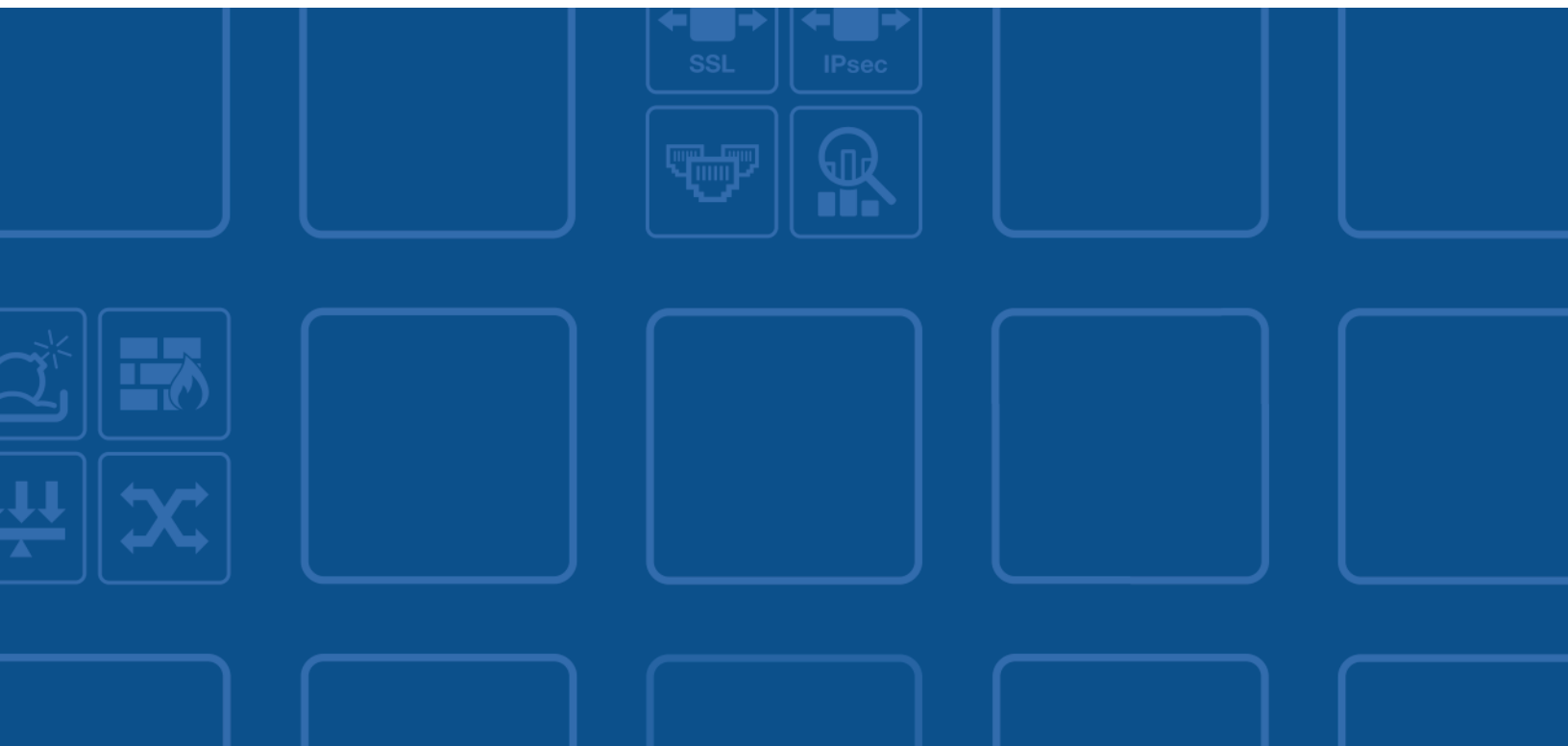
FORTINET
High Performance Network Security

# FortiAnalyzer - Administration Guide

VERSION 5.4.1



**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

November 23, 2016

FortiAnalyzer 5.4.1 Administration Guide

05-541-27931-20161123

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
|---|---|
| 2016-06-29 | Initial release |
| 2016-07-05 | Corrected the Allow Save Maximum value in Report Settings |
| 2016-07-11 | Updated the SNMP section |
| 2016-07-29 | Added the "Grouping reports" and "Validating datasets" sections |
| 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 identifies 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. Alerts and log information from Fortinet appliances and third-party devices are aggregated 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 FortiAnalyzerCommand 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 chapter provides a summary of the new features and enhancements in FortiAnalyzer.

## FortiAnalyzer 5.4.1

FortiAnalyzer 5.4.1 includes the following new features and enhancements.

### Security Service—Indicators of Compromise

Indicators of Compromise (IOC), a new, dynamically updated engine and signature service is now available for FortiAnalyzer. The IOC engine detects end users with suspicious web usage compromises by checking new and historical logs against the IOC signatures, which are based on your FortiGuard subscription. An IOC summary is available in FortiView. See Viewing end users' Indicators of Compromise (IOC) information on page 96.

### FortiView

#### Export a FortiView Summary to Chart

You can export a filtered FortiView summary, or any level of its drilldowns, to a custom chart. This new chart is saved in the chart library and can be inserted into reports. See Exporting filtered summaries to report charts on page 96.

#### JSON API Support

An extension of the JSON API allows remote systems to query and retrieve FortiView data.

#### FortiClient Vulnerability Detection

A new "Endpoints Vulnerabilities" FortiView summary is available for you to monitor FortiClient vulnerability detection and remediation. See FortiView summary list and description on page 88.

#### New FortiView Summaries for FortiClient EMS ADOM

The following FortiView summaries are now available for a FortiClient EMS ADOM: Top Threats, Top Applications, Top Websites, All Endpoints, and Endpoints Vulnerabilities. See FortiView summaries for FortiClient EMS devices on page 90.

#### Performance Optimization

FortiView performance is optimized with the addition of intelligent summaries and caching.

## Reports

### FortiClient Vulnerability Scan Report

FortiAnalyzer supports the new FortiClient 5.4.1 Vulnerability Scan feature by including a new "FortiClient Vulnerability Scan Report" report template, which summarizes all the FortiClient endpoints in the network, plus their installed applications and any vulnerabilities. See List of report templates on page 142.

### Report Generation Diagnostic Tool

When you start running a report, a log about the report generation status and system performance is created. The log breaks down the time taken to generate each chart in the report. You can use this log to troubleshoot report generation problems and tune the system. You can also download the diagnostic log. See Retrieving report generation logs on page 124.

## Log Forwarding

### Field Exclusion

You can now control which log fields to include when you forward logs to a remote Syslog or CEF server. See Configuring log forwarding on page 165.

## Log Fetching

Log fetching is a new feature in FortiAnalyzer 5.4. It enables you to run queries or reports against historical (archived) database for forensic analysis. The fetch client queries the remote FortiAnalyzer fetch server and retrieves the needed data. FortiAnalyzer 5.4.1 includes usability improvements for the setup and authentication between fetch client and server. See Log fetcher management on page 167.

## Log View

### Log Details in Tree View

Log fields in the details pane are now grouped in tree view for better readability. See Viewing log message details on page 101.

### Case-Insensitive Search

Search in Log View is now case-insensitive by default. See Filtering log messages on page 102.

# 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 22.

## 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 88.

## Report extensions

FortiAnalyzer includes the new reports, report templates, and charts. See Reports on page 121.

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 106.

## 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 Archive 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 many 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 Two operation modes on page 18, Archive logs and Analytics logs on page 20, and Log storage on page 20.

## Fetching

You can fetch offline, Archive 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 Archive 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 164.

## 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.

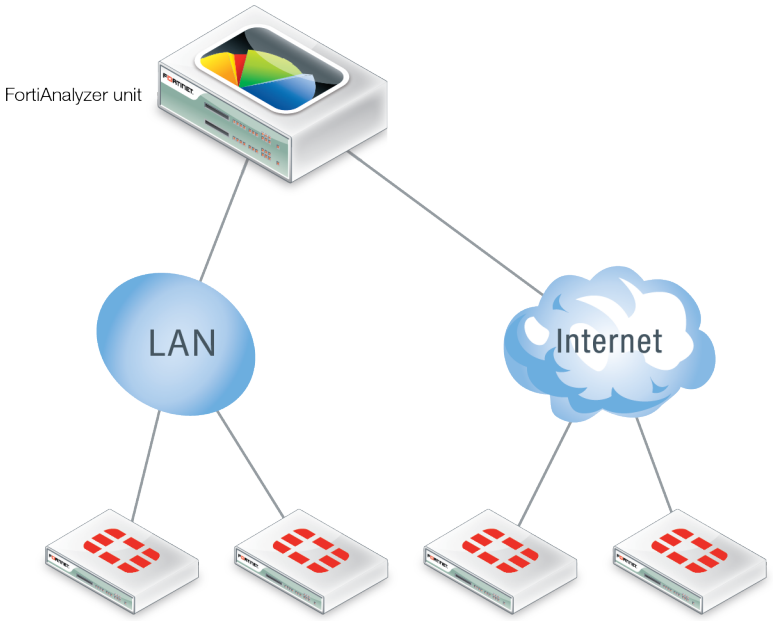
## Two operation modes

FortiAnalyzer provides two operation modes: Analyzer and Collector. Choose the operation mode for your FortiAnalyzer units based on your network topology and individual requirements.

### Analyzer mode

The Analyzer mode is the default mode that supports all FortiAnalyzer features, such as *FortiView*, *Event Monitor*, and *Reports*. You can use this mode to aggregate logs from one or more Collectors.

The following diagram illustrates an example of deploying a FortiAnalyzer unit in Analyzer mode.




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

### Collector mode

When a FortiAnalyzer is configured to work in the Collector mode, its primary task becomes forwarding logs of the connected devices to an Analyzer and archiving the logs. Instead of writing logs to the database, the Collector retains the logs in their original (binary) format for uploading. In this mode, most features, including *FortiView, Event Monitor*, and *Reports*, are disabled.

### Analyzer and Collector: Feature comparison

| 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 |

### Analyzer–Collector collaboration

You can deploy the Analyzer mode and Collector mode on different FortiAnalyzer units and make the units work together to improve the overall performance of log receiving, analysis, and reporting. The Collector offloads the log receiving task from the Analyzer so that the Analyzer can focus on data analysis and report generation. Since collecting logs from the connected devices is the dedicated task of the Collector, its log receiving performance is maximized.

For an example of setting up Analyzer–Collector collaboration, see Configuring Analyzer–Collector collaboration on page 28.

## 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 43. For information on configuring administrator accounts, See Administrator Accounts on page 51.

ADOMs must be enabled to support FortiCarrier, FortiClient EMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox logging and reporting. See Administrative Domains on page 43.

# 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 88, Log View on page 99, and Reports on page 121.

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 Two operation modes on page 18.

## Archive logs and Analytics 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:

- Archive logs: Compressed on hard disks and offline
- Analytics logs: 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 Archive logs and how long to keep Analytics logs 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 Archive logs on the FortiAnalyzer disks

  When the specified amount of time in the data policy expires, Archive logs are deleted from the FortiAnalyzer disks.

See also Configuring log storage policy on page 79.

## Disk utilization for compressed and Analytics 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 Analytics and Archive 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 policy on page 79.

# 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.

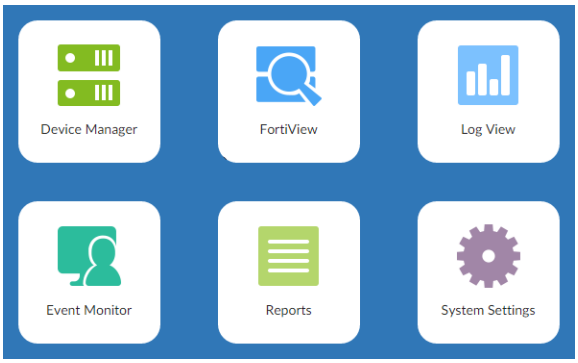
For information on enabling administrative access protocols and configuring IP addresses, see Configuring ports and administrator access on page 31.

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 32.

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 53.

## 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.

| | |
|---|---|
| **Device Manager** | Add and manage devices and VDOMs. See Devices on page 68. |
| **FortiView** | 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.<br>For each summary view, you can drill down into details for the event. See FortiView on page 88.<br>This pane is not available when the unit is in Collector mode. See Two operation modes on page 18 |
| **Log View** | 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 groups. See Log View on page 99.<br>This pane is not available when the unit is in Collector mode. See Two operation modes on page 18 |
| **Event Monitor** | Configure and view events for managed log devices.See Event Monitor on page 110.<br>This pane is not available when the unit is in Collector mode. See Two operation modes on page 18 |
| **Reports** | Generate reports. You can also configure report templates, schedules, and output profiles, and manage charts and datasets. See Reports on page 121.<br>This pane is not available when the unit is in Collector mode. See Two operation modes on page 18 |
| **System Settings** | Configure system settings, such as network interfaces, administrators, system time, server settings, and others. You can also perform maintenance and firmware operations. See System Settings on page 151. |

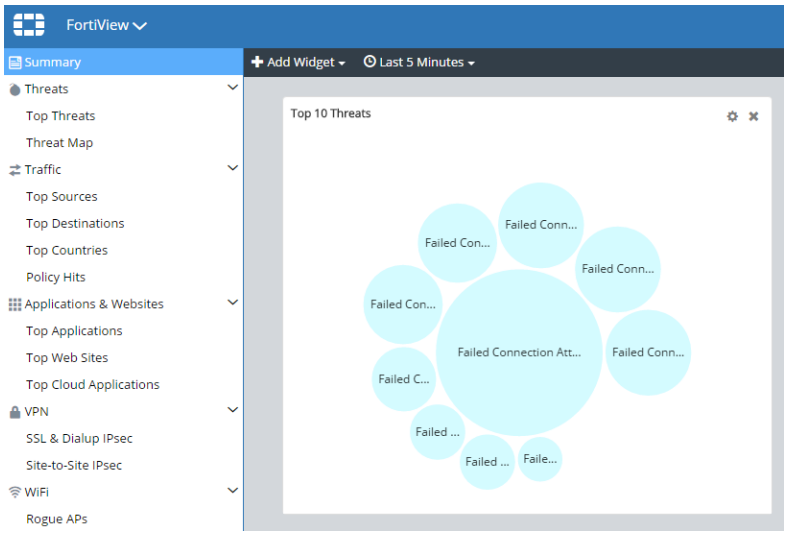
The top-right corner of the home page includes an *admin* menu, as well as a *Notification* button, and a *Help* button.

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

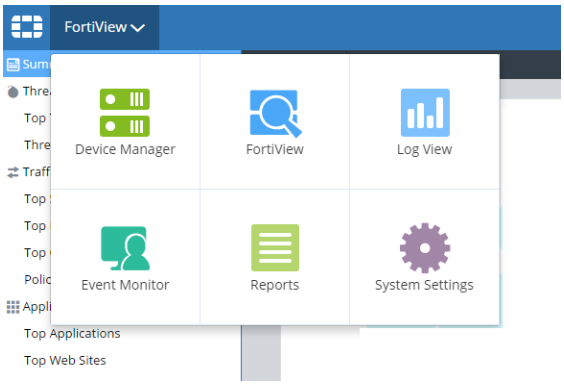
## Panes

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

| | |
|---|---|
| **Banner** | Along the top of the page; includes the home button (Fortinet logo), tile menu, ADOM menu (when enabled), admin menu, notifications, and help button. |
| **Tree menu** | On the left side of the screen; includes the menus for the selected pane. Not available in *Device Manager*. |
| **Content pane** | 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. |
| **Toolbar** | Directly above the content pane; includes options for managing content in the content pane, such as *Create New* and *Delete*. |

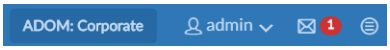



To switch between panes, either select the home button to return to the home page, or select the tile menu then select a new tile.




## Switching between ADOMs

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

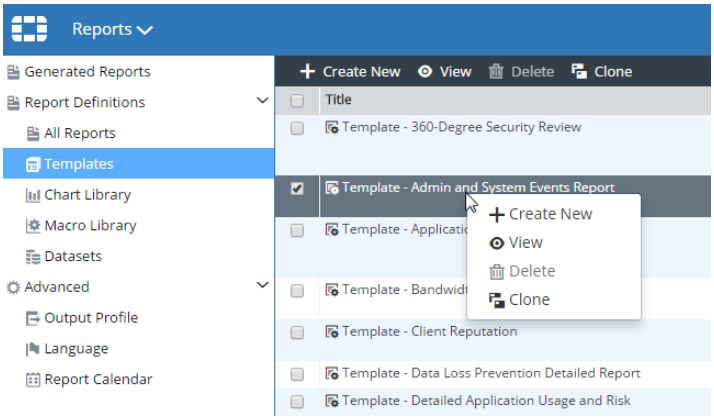



ADOM access is controlled by administrator accounts and the profile assigned to the administrator account. Depending on your account privileges, you might not have access to all ADOMs. See also Administrator Accounts on page 51.

## 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.

# Getting started

This chapter provides information about performing some basic setups for your FortiAnalyzer units.

## Target audience and access level

This guide is intended 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 some tasks described in this guide. For more information about administrator profiles, see Administrator profiles on page 52.

If you logged in by using the `admin` administrator account, you have the *Super_User* administrator profile, which is assigned to the *admin* account by default and gives the `admin` administrator full privileges.

## Initial Setup

This topic provides an overview of the tasks that you need to do to get your FortiAnalyzer unit up and running.

**To set up FortiAnalyzer:**

1. Connect to the GUI. See Connecting to the GUI on page 22.
2. Configure the RAID level, if the FortiAnalyzer unit supports RAID. See Configuring RAID on page 39.
3. Configure network settings. See Configuring ports and administrator access on page 31.

Once the IP address of the administrative port of FortiAnalyzer is changed, you will lose connection to FortiAnalyzer. You will have to reconfigure the IP address of the management computer to connect again to FortiAnalyzer and continue.

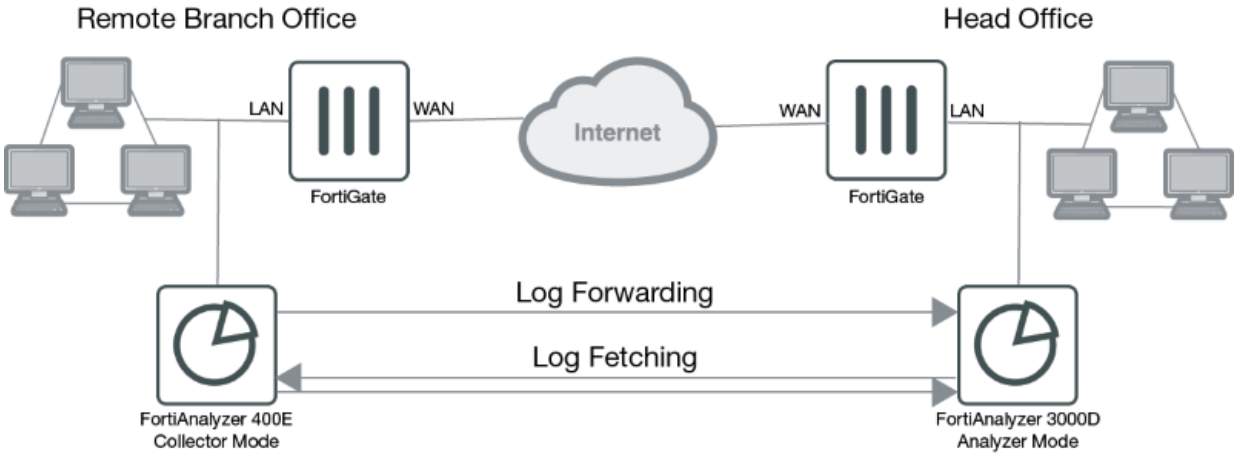
4. (Optional) Configure administrative domains. See Configuring ADOMs on page 44.
5. Configure administrator accounts. See Configuring administrator accounts on page 53.

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

6. Add devices to the FortiAnalyzer unit so that the devices can send logs to the FortiAnalyzer unit. See Adding devices on page 69.
7. Configure the operation mode. See Configuring operation modes on page 155 and Two operation modes on page 18.

# Configuring Analyzer–Collector collaboration

This topic describes how to configure two FortiAnalyzer units as the Analyzer and Collector respectively and make them work together. In this scenario (as shown in the following diagram), Company A has a remote branch network with a FortiGate unit and a FortiAnalyzer 400E in the Collector mode deployed. In its head office, Company A has another FortiGate unit and a FortiAnalyzer 3000D in the Analyzer mode deployed. The Collector forwards the logs of the FortiGate unit in the remote branch to the Analyzer in the head office for data analysis and reports generation. The Collector will also be used for log archival.




For the related concepts, see Two operation modes on page 18 and Analyzer–Collector collaboration on page 19. You need to complete the initial setup for your FortiAnalyzer units first. See "Initial Setup" on page 27.

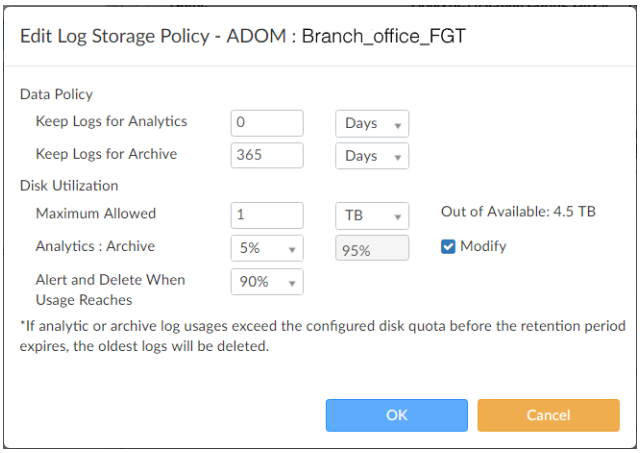
## Configuring the Collector

**To configure the Collector:**

1. If you have not done it yet, set the Operation Mode to *Collector*. See Configuring operation modes on page 155
2. Check and configure the storage policy for the Collector. See Monitoring log storage policy on page 81 and Configuring log storage policy on page 79.

For the Collector, you should allocate most of the disk space for Archive logs. You should keep the Archive logs long enough to meet the regulatory requirements of your organization. After this initial configuration, you can monitor the storage usage and adjust it as you go.

Following is a storage configuration example of the Collector.




3. Set up log forwarding to enable the Collector to forward the logs to the Analyzer. See Log Forwarding on page 164. In particular,
   - Set *Remote Server Type* to *FortiAnalyzer*.
   - Set *Server IP* to the IP address of the Analyzer that this Collector will forward logs to.
   - Click *Select Device* and select the FortiGate device that the Collector will forward logs for.

Per the default setting, the Collector will forward logs in real time to the Analyzer. If you want the Collector to upload *content files*, which include DLP (data leak prevention) files, antivirus quarantine files, and IPS (intrusion prevention system) packet captures, you should set the log forwarding mode to *Both* so that the Collector will also send content files to the Analyzer daily at the scheduled time. See Configuring log forwarding mode in CLI on page 165.

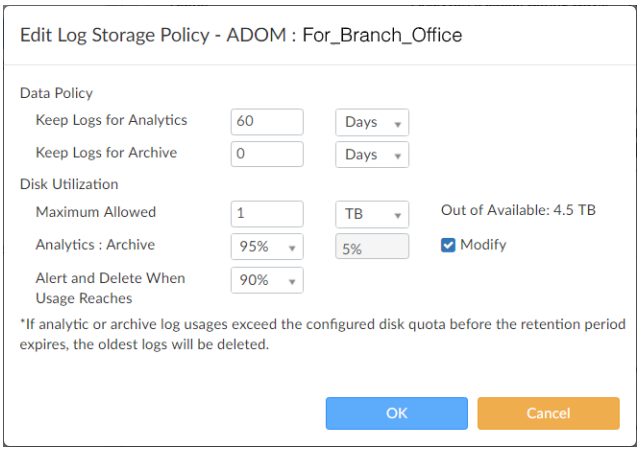
## Configuring the Analyzer

**To configure the Analyzer:**

1. (Only when necessary) Set the Operation Mode to *Collector*. See Configuring operation modes on page 155
2. Check and configure the storage policy for the Analyzer. See Monitoring log storage policy on page 81 and Configuring log storage policy on page 79.

For the Analyzer you should allocate most of the disk space for Analytics logs. You may want to keep the Analytics logs for 30–90 days. After this initial configuration, you can monitor the storage usage and adjust it as you go.

Following is a storage configuration example of the Analyzer.




3. Make sure that the aggregation service is enabled on the Analyzer. If not, use this CLI command to enable it:

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

4. Add the FortiGate device of the remote office that the Collector will forward logs for. See Adding devices manually on page 71.

   Once the FortiGate of the remote office is added, the Analyzer starts receiving its logs from the Collector.

## Fetching logs from the Collector to the Analyzer

At times, you might want to fetch logs from the Collector to the Analyzer. The Collector will perform the role of the fetch server, and the Analyzer will perform the role of fetch client. For information about how to conduct log fetching, see Conducting log fetching between two FortiAnalyzer units on page 167.

# Next steps

Now that you have set up your FortiAnalyzer units and they have started receiving logs from the devices, you can start monitoring and interpret data. You can:

- View log messages collected by the FortiAnalyzer unit in *Log View*. See Log View on page 99.
- View summaries of threats, traffic, and more in *FortiView* . See FortiView on page 88
- Generate and view events in *Event Monitor*. See Event Monitor on page 110.
- Generate and view reports in *Reports*. See Reports on page 121.

# 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 statics 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, 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 51 and Configuring administrator accounts on page 53.

## Configuring the network

### Configuring ports and administrator access

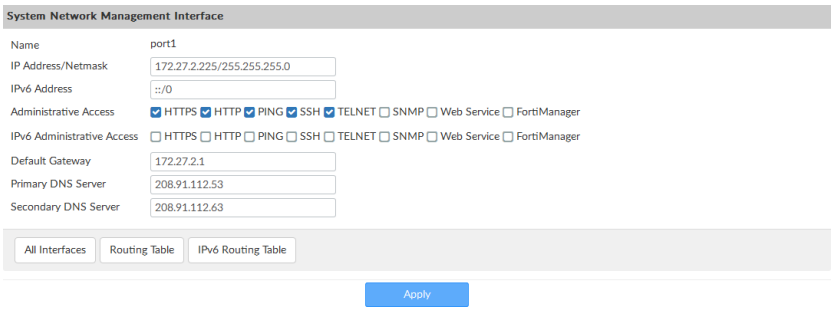
The following port configuration is recommended:

- 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 33.




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 34.
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 34.
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: *HTTPS*, *HTTP*, *PING*, *SSH*, *TELNET*, *SNMP*, *Web Service*, and *FortiManager*. |
| IPv6 Administrative Access | Select the allowed IPv6 administrative service protocols from: *HTTPS*, *HTTP*, *PING*, *SSH*, *TELNET*, *SNMP*, *Web Service*, and *FortiManager*. |
| 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. |
| Alias | Type an alias for the port to make it easily recognizable. |
| IP Address/Netmask | Type the IP address and netmask for the interface. |

| Field | Description |
|---|---|
| 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 *Enable* to enable the interface and allow the interface to accept network traffic. Click *Disable* 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-200D | NA | NA | NA |
| FAZ-300D | Software RAID | Linear, 0, 1 | No |

| Model | RAID Type | RAID Level | Hot Swappable |
|---|---|---|---|
| FAZ-400E | Software RAID | Linear, 0,1,1s,5,5s,10 | No |
| FAZ-1000D | Hardware RAID | 0, 1, 5, 10 | Yes |
| FAZ-1000E | Hardware RAID | 0,1,1s, 5,5s, 6, 6s, 10, 50, 60 | Yes |
| FAZ-2000B | Hardware RAID | 0,1,1s, 5,5s, 6, 6s, 10, 50 | Yes |
| FAZ-2000E | Hardware RAID | 0,1,1s, 5,5s, 6, 6s, 10, 50, 60 | Yes |
| FAZ-3000D | Hardware RAID | 0,1,1s, 5,5s, 6, 6s, 10, 50, 60 | Yes |
| FAZ-3000E | Hardware RAID | 0,1,1s, 5,5s, 6, 6s, 10, 50, 60 | Yes |
| FAZ-3000F | Hardware RAID | 0,1,1s, 5,5s, 6, 6s, 10, 50, 60 | Yes |
| FAZ-3500E | Hardware RAID | 0,1,1s, 5,5s, 6, 6s, 10, 50, 60 | Yes |
| FAZ-3500F | Hardware RAID | 0,1,1s, 5,5s, 6, 6s, 10, 50, 60 | Yes |
| FAZ-3900E | Hardware RAID | 0,1,1s, 5,5s, 6, 6s, 10, 50, 60 | Yes |
| FAZ-4000B | Hardware RAID | 0,5,5s, 6, 6s, 10, 50, 60 | Yes |

## 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

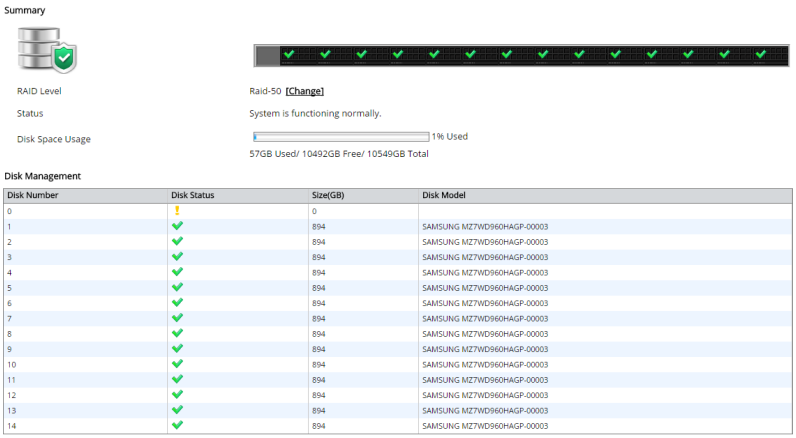
You can monitor RAID status, swap hard disks, and in some cases, add new disks to the FortiAnalyzer unit.

## 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 and updating FortiAnalyzer firmware 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 41.




## 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 and updating FortiAnalyzer firmware 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 25), install the disk or disks, and then restart the device.
4. Configure the RAID level. See Configuring RAID on page 39.
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 |
|---|---|
| **Summary** | Displays summary information about the RAID array. |
| **Graphic** | Displays the position and status of each disk in the RAID array. Hover over each disk to view status details. |
| **RAID Level** | Displays the selected RAID level. Click *Change* to change the selected RAID level. When you change the RAID settings, all data is deleted. |

| Field | Description |
|---|---|
| **Status** | Displays the overall status of the RAID array |
| **Disk Space Usage** | Displays the total size of the disk space, how much disk space is used, and how much disk space is free. |
| **Disk Management** | Displays information about each disk in the RAID array. |
| **Disk Number** | Identifies the disk number for each disk in the RAID array |
| **Disk Status** | Displays the status of each disk in the RAID array<br>• *Ready*: The hard drive is functioning normally.<br>• *Rebuilding*: The FortiAnalyzer unit is writing data to a newly added hard drive in order to restore the hard drive to an optimal state. The FortiAnalyzer unit is not fully fault tolerant until rebuilding is complete.<br>• *Initializing*: The FortiAnalyzer unit is writing to all the hard drives in the device in order to make the array fault tolerant.<br>• *Verifying*: The FortiAnalyzer unit is ensuring that the parity data of a redundant drive is valid.<br>• *Degraded*: The hard drive is no longer being used by the RAID controller.<br>• *Inoperable*: One or more drives are missing from the FortiAnalyzer unit. The drive is no longer available to the operating system. Data on an inoperable drive cannot be accessed. |
| **Size (GB)** | Displays the size in GB of each disk in the RAID array |
| **Disk Model** | 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 mange. 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 the logging and reporting of non-FortiGate devices, such as FortiCarrier, FortiClient EMS, FortiMail, FortiWeb, FortiCache, and FortiSandbox. When a non-FortiGate device is registered with a FortiAnalyzer unit, the device is added to its respective default ADOM..

### 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 25.

### 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 on the FortiGate device. When endpoints are registered to a FortiClient EMS server, you view FortiClient logs by viewing the FortiClient ADOM that the FortiClient EMS device is added to. 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 45.

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:

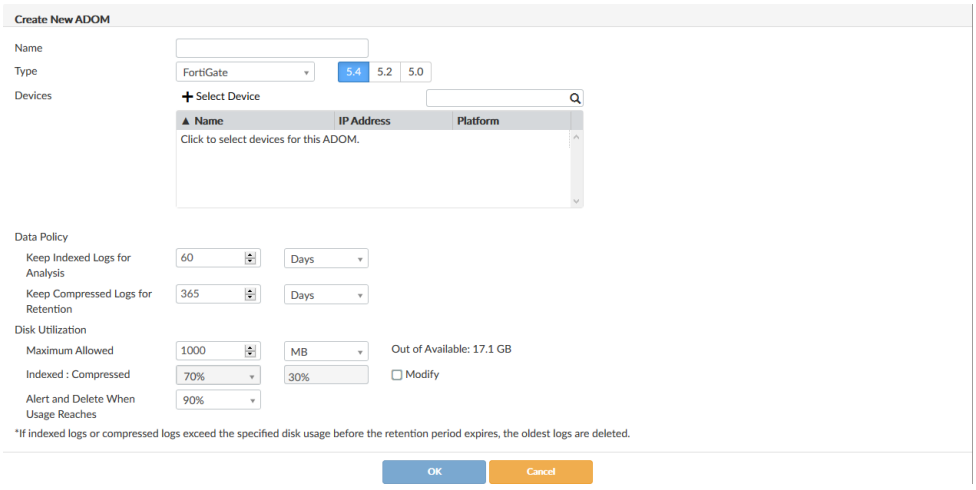
```
config system global
   set adom-mode {normal | advanced}
end
```

## 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 Archive 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(Edit) ADOM dialog box on page 46.




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

### Create(Edit) ADOM dialog box

Following is a description of the options available on the *Create(Edit) ADOM* dialog box.

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

| Field | Description |
|---|---|
| **Name** | Displays the name of the selected ADOM. Type a new name to create a new ADOM. |
| **Data Policy** | Use the *Data Policy* settings to specify how long to keep logs in the indexed and compressed states. |
| **Keep Logs for Analytics** | 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 *FortiView*, *Event Monitor*, and *Reports* tabs. After the specified amount of time expires, logs are automatically purged from the SQL database. |
| **Keep Logs for Archive** | 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 *FortiView*, *Event Monitor*, and *Reports* tabs. After the specified amount of time expires, Archive logs are automatically deleted from the FortiAnalyzer unit. |
| **Disk Utilization** | Use the *Disk Utilization* settings to specify how much FortiAnalyzer disk space to use for logs. |
| **Maximum Allowed** | 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 FortiAnalyzer disk space allocation on page 75. |
| **Analytics: Archive** | Specify how much of the allotted space to use for Analytics and Archive logs. Analytics logs require more space than Archive logs. For example, a setting of 70% and 30% indicates that 70% of the allotted disk space will be used for Analytics logs, and 30% of the allotted space will be used for Archive logs. Select the *Modify* check box to change the setting. |
| **Alert and Delete When Usage Reaches** | Specify at what fullness you want alert messages to be generated and logs to be automatically deleted. The oldest Archive log files or Analytics database tables are deleted first. |

## 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 45.

**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 |
|---|---|
| **Create New** | Create a new ADOM |
| **Edit** | Edit the selected ADOM. |
| **Delete** | Deletes the selected ADOM. You cannot delete default ADOMs, such as the root. |
| **Switch to ADOM** | Switches to ADOM. |
| **Expand Devices** | Expands the ADOM to show the device list within the ADOM. |
| **Collapse Devices** | 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.

| Field | Description |
|---|---|
| **Name** | Displays the name of the ADOM. ADOMs are listed in the following groups: *Central Management* and *Other Device Types*. You can expand and hide the groups to view the ADOMs contained in the group. |
| **Firmware Version** | Displays the version of devices the ADOM contains. |
| **Allocated Storage** | The amount of hard drive storage space allocated to the ADOM. |
| **Device** | 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. |
|  | 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

# 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:

| | |
|---|---|
| **Restricted_User** | Restricted user profiles have no System Privileges enabled, and have read-only access for all Device Privileges. |
| **Standard_User** | Standard user profiles have no System Privileges enabled, but have read/write access for all Device Privileges. |
| **Super_User** | Super user profiles have all system and device privileges enabled. 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 / `system-setting` | Read-Write | None | None |
| Administrator Domain / `adom-switch` | Read-Write | Read-Write | None |
| Device Manager / `device-manager` | Read-Write | Read-Write | Read-Only |
| Add/Delete Devices/Groups / `device-op` | Read-Write | Read-Write | None |
| FortiView / `realtime-monitor` | Read-Write | Read-Write | Read-Only |
| Event Management / `event-management` | Read-Write | Read-Write | Read-Only |
| Reports / `report-viewer` | 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.

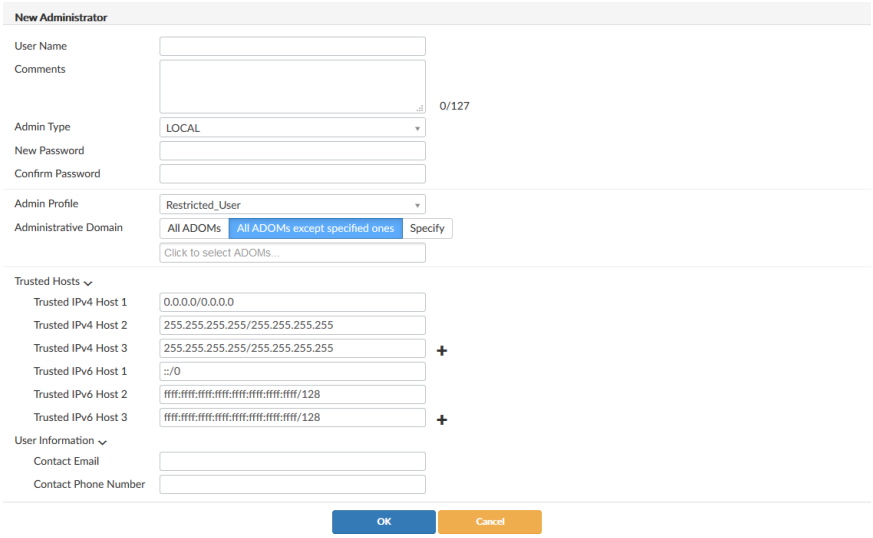
## Configuring administrator accounts

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 65.




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 |
|---|---|
| **Create New** | Create a new administrator account. |
| **Edit** | Edit the selected administrator account. |
| **Delete** | Delete the selected administrator account. You cannot delete the default *admin* administrator account from the GUI. |

## Viewing administrator accounts

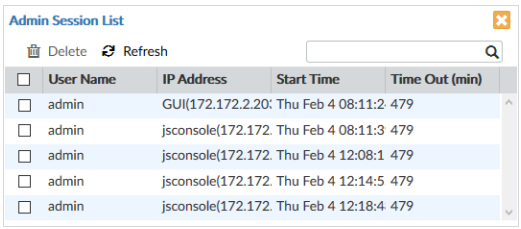
Go to *System Settings* > *Admin* > *Administrator* to view the list of administrators. Only the default `admin` administrator account can see the complete administrators list. If you do not have certain viewing privileges, you will not see the administrator list.

## 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.




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 |
|---|---|
| **Create New** | Create a new administrator profile. |
| **Edit** | Edit an administrator profile.The *Super_User* profile cannot be deleted. |
| **Delete** | 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: *Restricted_User*, *Standard_User*, and *Super_User*. |

## 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 66.
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 |
|---|---|
| **Create New** | Create a new remote authentication server. |
| **Edit** | Edit a remote authentication server. You cannot change the name field when editing a remote authentication server. |
| **Delete** | Delete the selected remote authentication server. You cannot delete a remote authentication server entry if administrators are using it. |

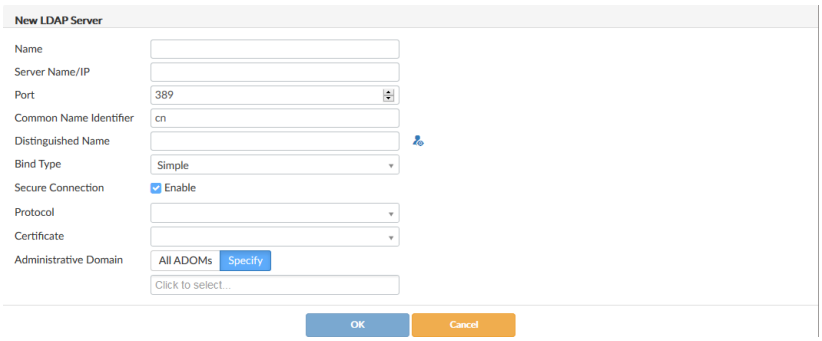
## Adding an LDAP server

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.




3. Configure the following information:

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

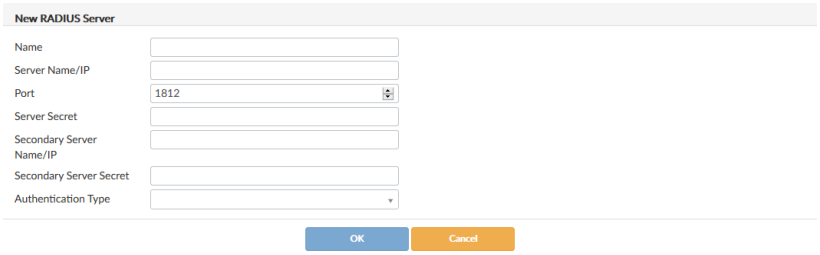
## Adding a RADIUS server

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:

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

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

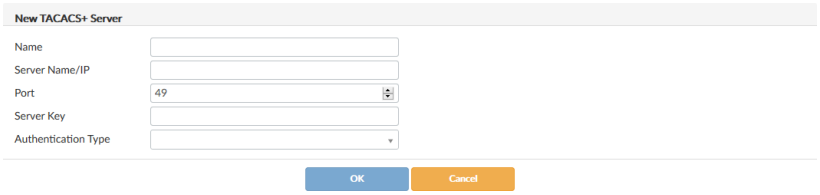
## Adding a TACACS+ server

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.




3. Configure the following information:

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

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.

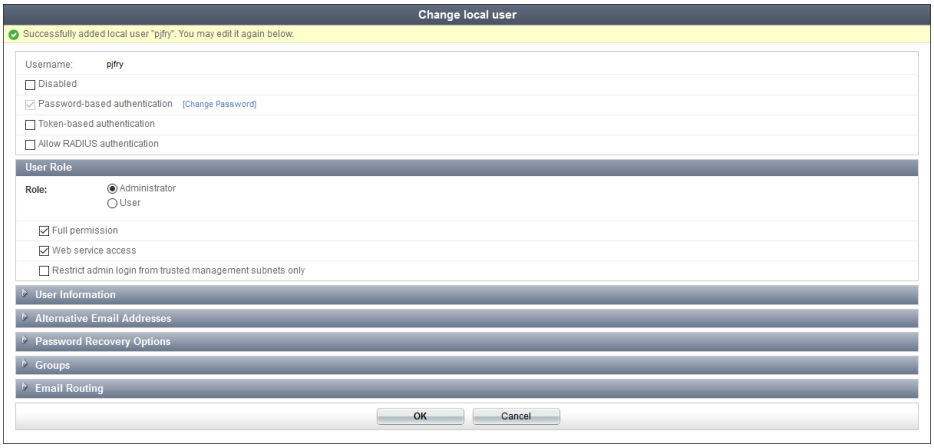
Before proceeding, ensure that you have configured your FortiAuthenticator and that you have created a NAS entry for your FortiAnalyzer and created/imported FortiTokens. For more information, see the *FortiAuthenticator Interoperability Guide* and *FortiAuthenticator Administration Guide* available in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

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

4. Select *OK* to continue.




5. Configure the following settings:

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

| | | |
|---|---|---|
| **Enable account expiration** | | Optionally, select to enable account expiration. For more information see the *FortiAuthenticator Administration Guide*. |
| **User Role** | | |
| **Role** | | Select either *Administrator* or *User*. |
| | **Full Permission** | Select to allow Full Permission, otherwise select the admin profiles to apply to the user. This option is only available when *Role* is *Administrator*. |
| | **Web service** | 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 *Role* is *Administrator*. |
| | **Restrict admin login from trusted management subnets only** | Select to restrict admin login from trusted management subnets only, then enter the trusted subnets in the table. This option is only available when *Role* is *Administrator*. |
| | **Allow LDAP Browsing** | Select to allow LDAP browsing. This option is only available when *Role* is *User*. |

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:

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

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

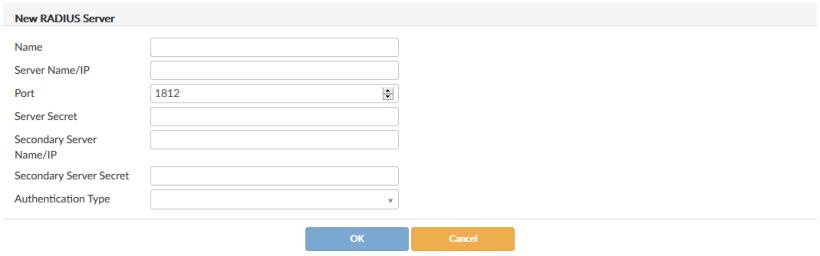
4. Select *OK* to save the setting.

## 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.




3. Configure the following settings:

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

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 58.
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.

# Admin settings

In the Admin Settings pane, you can configure administration settings, password policy, GUI language, and GUI theme.

Only administrators with the *Super_User* profile can access and configure admin settings. The admin settings is global and applies to all the administrators of the FortiAnalyzer unit.

## Configuring administration settings

**To configure administration settings:**

1. Go to *System Settings* > *Admin* > *Admin Settings*.
2. Configure the Administration Settings.

| Field | Description |
|---|---|
| **HTTP Port** | Enter the TCP port to be used for administrative HTTP access. Select *Redirect to HTTPS* to redirect HTTP traffic to HTTPS. |
| **HTTPS Port** | Enter the TCP port to be used for administrative HTTPS access. |
| **HTTPS & Web Service Server Certificate** | Select a certificate from the drop-down list. |
| **Idle Timeout** | Enter the number of minutes that an administrative connection can be idle before the administrator must log in again. The maximum is 480 minutes (8 hours).<br><br>**Note**: To ensure security, the idle timeout should be a short period of time to prevent the administrator from inadvertently leaving the management computer logged-in and unattended. |

3. Click *Apply*.

## Configuring password policy

You can enable password and configure password policy for your FortiAnalyzer.

**To configure administrative settings:**

1. Go to *System Settings* > *Admin* > *Admin Settings*.
2. Go to *Password Policy*, and select *Enable*.
3. Configure the password policy.

| | |
|---|---|
| **Minimum Length** | Specify the minimum length of a password. The default is eight characters. |
| **Must Contain** | Specify the types of characters that a password must contain. |
| **Admin Password Expires after** | Specify the number of days that a password is valid for, after which time it must be changed. |

4. Click *Apply*.

## Configuring 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 set 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. For more information about FortiAnalyzer language support, see FortiAnalyzer5.4.1 Release Notes.

**To configure 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. Click *Apply*.

## Picking a GUI theme

In addition to the default blue GUI theme, FortiAnalyzer provides other themes for you to choose from.

**To pick a GUI theme:**

1. Go to *System Settings* > *Admin* > *Admin Settings*.
2. Go to *Theme*, and click a theme to select it. A preview of the theme is displayed.
3. Click *Apply*.

# 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 |
|---|---|
| **User Name** | Enter the name that this administrator uses to log in. |
| **Comments** | 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. |
| **Admin Type** | Select the type of authentication the administrator will use when logging into the FortiAnalyzer unit. Select one of: *LOCAL*, *RADIUS*, *LDAP*, *TACACS+*, or *PKI*. |
| **Server** | Select the *RADIUS*, *LDAP*, or *TACACS+* server, as appropriate. This option is only available if *Admin Type* is not *LOCAL* or *PKI*. |
| **Wildcard** | Select this option to set the password as a wildcard. This option is only available if *Admin Type* is not *LOCAL* or *PKI*. |
| **Subject** | If *Admin Type* is set to *PKI*, enter a description. |
| **CA** | If *Admin Type* is set to *PKI*, select a certificate in the drop-down list. |
| **Require two-factor authentication** | If *Admin Type* is set to *PKI*, you can select the check box to enforce two-factor authentication. |
| **New Password** | Enter the password.<br>This option is not available if *Wildcard* is selected.<br>If *Admin Type* is *PKI*, this option is only available when *Require two-factor authentication* is selection. |
| **Confirm Password** | Enter the password again to confirm it.<br>This option is not available if *Wildcard* is selected.<br>If *Admin Type* is *PKI*, this option is only available when *Require two-factor authentication* is selection. |
| **Admin Profile** | Select a profile from the list. The profile selected determines the administrator's access to the FortiAnalyzer unit's features.<br>*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. |

| Field | Description |
|---|---|
| **Administrative Domain** | Choose the ADOMs this administrator will be able to access, select *All ADOMS*, *All ADOMs except specified ones* or *Specify*. Select the remove icon to remove an ADOM.<br>This field is available only if ADOMs are enabled.The *Super_User* profile can only be set to *All ADOMs*. |
| **Trusted Host** | 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.<br>Setting trusted hosts for all of your administrators can enhance the security of your system. |
| **User Information** | 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 |
|---|---|
| **Profile Name** | Enter a name for this profile. |
| **Description** | Enter a description for this profile. While not a requirement, a description can help to know what the profiles is for or the levels it is set to. |
| **Other Settings** | Select *None*, *Read Only*, or *Read-Write* access for 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 |
|---|---|
| **HTTP Port** | Enter the TCP port to be used for administrative HTTP access. Select *Redirect to HTTPS* to redirect HTTP traffic to HTTPS. |
| **HTTPS Port** | Enter the TCP port to be used for administrative HTTPS access. |
| **HTTPS & Web Service Server Certificate** | Select a certificate from the drop-down list. |

| Field | Description |
|---|---|
| **Idle Timeout** | Enter the number of minutes that an administrative connection can be idle before the administrator must log in again. The maximum is 480 minutes (8 hours). To ensure security, the idle timeout should be a short period of time to avoid the administrator inadvertently leaving the management computer logged in to the FortiAnalyzer unit, creating the possibility of someone walking up and modifying the network options. |
| **Language** | Select a language from the drop-down list. Select either *English*, *Simplified Chinese*, *Traditional Chinese*, *Japanese*, *Korean*, or *Auto Detect*. The default value is *Auto Detect*. |
| **Password Policy** | Select to enable a password policy for all administrators. |
| **Minimum Length** | Select the minimum length for a password. The default is eight characters. |
| **Must Contain** | Select the types of characters that a password must contain. |
| **Admin Password Expires after** | Select the number of days that a password is valid for, after which time it must be changed. |

# 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 164.

### How ADOMs affect devices

When ADOMs are enabled, the *Device Manager* pane is displayed per ADOM. See also Switching between ADOMs on page 25.

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 44.

### 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.

## The quick status bar


You can see the quick status bar at the top of the *Device Manager* pane. The quick status bar contains the following tabs:

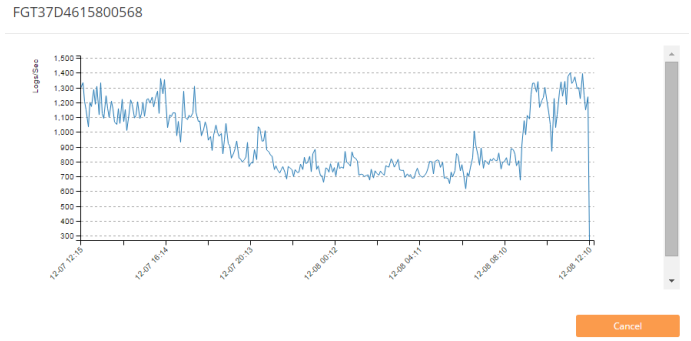
- *Devices Total*: Displays the registered devices.
- *Devices Unregistered*: Displays the unregistered devices.
- *Devices Log Status Down*: Displays the registered devices with a log status of down.
- *Storage Used*: Displays the *Log View* > *Storage Statistics* page.

## 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.

## Connecting to a registered device GUI

You can connect to the GUI of a registered device from *Device Manager*.

**To connect to a registered device GUI:**

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to the *Device Manager*, and click the *Devices Total* tab in the quick status bar.
3. Right-click the device that you want to access, and select *Connect to Device*.

You will be directed to the Login page of the device GUI.

# 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.

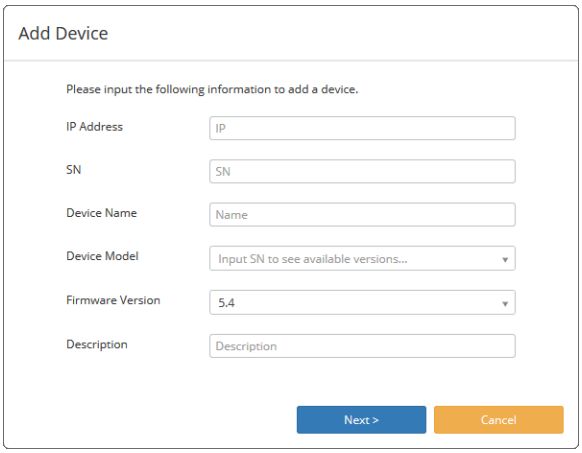
## Adding devices using the wizard

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:**

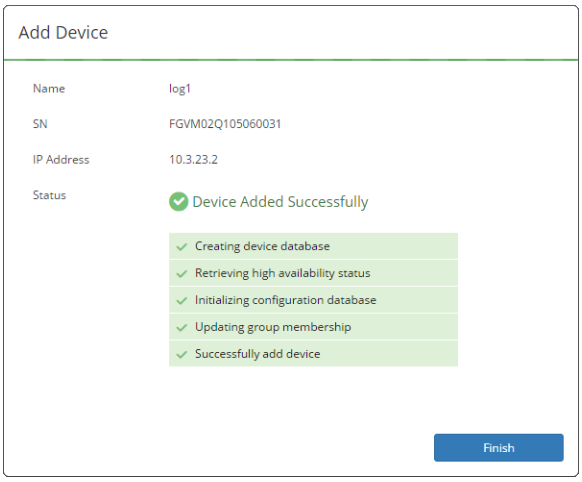
1. If ADOMs are enabled, ensure you are working in the ADOM to which the device will be added. Otherwise skip this step.
2. Go to *Device Manager* and click *Add Device*.

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




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.




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.

# Device references

## 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 |
|---|---|
| **Device Name** | Displays the name of the device. |
| **IP Address** | Displays the IP address for the device. |
| **Platform** | Displays the platform for the device. |
| **Logs** | 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.<br>A lock icon displays when a secure tunnel is being used to transfer logs from the device to the FortiAnalyzer unit. |
| **Average Log Rate (log/sec)** | 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. |

| Column | Description |
|---|---|
| **Device Storage** | Displays how much of the allotted disk space has been consumed by logs. |
| **Description** | Displays a description of the device. |

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

| Button | Description |
|---|---|
| **Add Device** | Opens the *Add Device Wizard* 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 *Unregistered Devices* tree menu. |
| **Edit** | Edit the selected device. |
| **Delete** | Click to deleted the selected device from the FortiAnalyzer unit. |
| **Column Settings** | Click the *Column Settings* menu, and select the columns that you want to display in the content pane. Select *Reset to Default* to display the default columns. |
| **More** | Click the *More* menu, and select *Import Device List* or *Export Device List*. |
| **Search** | 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 |
|---|---|
| **Device Name** | Displays the name of the device. |
| **Model** | Displays the model of the device. |
| **Serial Number** | Displays the serial number for the device. |
| **Connecting IP** | Displays the IP address for the device |

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

| Button | Description |
|---|---|
| **Add** | Click to register the selected device with the FortiAnalyzer unit, which enables the FortiAnalyzer unit to receive logs from the device. |
| **Delete** | 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 |
|---|---|
| **IP Address** | Type the IP address for the device. |
| **SN** | Type the serial number for the device. |
| **Device Name** | Type a name for the device. |
| **Device Model** | Select the model of the device. |
| **Firmware Version** | Select the firmware version of the device. |
| **Description** | Type a description of the device (optional). |
| **Next** | Click to proceed to the next screen. |
| **Cancel** | Click to cancel the wizard. |

## Edit Device pane

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

| Field | Description |
|---|---|
| **Name** | Displays the name of the device added to the FortiAnalyzer unit. |
| **Description** | Displays a description of the device. |
| **Company/Organization** | Displays the name of the company or organization that owns the device. |
| **Country** | Displays the name of the country where the device resides. |
| **Province/State** | Displays the name of the province or state where the device resides. |
| **City** | Displays the name of the city where the device resides. |
| **Contact** | Displays the contact information for the device. |
| **Geographic Coordinates** | This section displays the latitude and longitude coordinates for the device. |
| **Latitude** | Displays the latitude of the device location to support the interactive map on the *FortiView >Summary > Threats > Threat Map* pane. |

| Field | Description |
|---|---|
| **Longitude** | Displays the longitude of the device location to support the interactive map on the *FortiView >Summary > Threats > Threat Map* pane. |
| **IP Address** | Displays the IP address for the device. |
| **Admin User** | Displays the admin login for the device. |
| **Password** | Displays the password for the admin login. |
| **Device Information** | This section displays the serial number, device model, and firmware version for the device. |
| **Serial Number** | Displays the serial number for the device. |
| **Device Model** | Displays the model of the device |
| **Firmware Version** | Displays the firmware version of the device. |
| **HA Cluster** | Displays whether the device is part of a high-availability pair. Select to identify the device as part of an HA pair, and the identify the other device in the HA pair. |
| **Secure Connection** | Select to enable a secure connection between the device and the FortiAnalyzer unit. |
| **ID** | Displays the ID for the device. |
| **Pre-Shared Key** | Enter the pre-shared key for the device. |
| **Device Permissions** | 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 |
|---|---|
| **Small Disk (less than 500GB)** | The system reserves either 20% or 50GB of disk space, which ever is smaller. |
| **Medium Disk (less than 1000GB)** | The system reserves either 15% or 100GB of disk space, which ever is smaller. |
| **Large Disk (less than 3000GB)** | The system reserves either 10% or 200GB of disk space, which ever is smaller. |
| **Very Large Disk (less than 5000GB)** | 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 Archive 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 Archive 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 Archive 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 Archive logs for each device. When the specified amount of time expires, Archive 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 Archive 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, Archive logs for the affected device are automatically deleted. Conversely, if the global automatic file deletion policy hits its threshold first, the oldest Archive logs on the FortiAnalyzer unit, regardless of the log storage settings associated with the device, are automatically deleted.

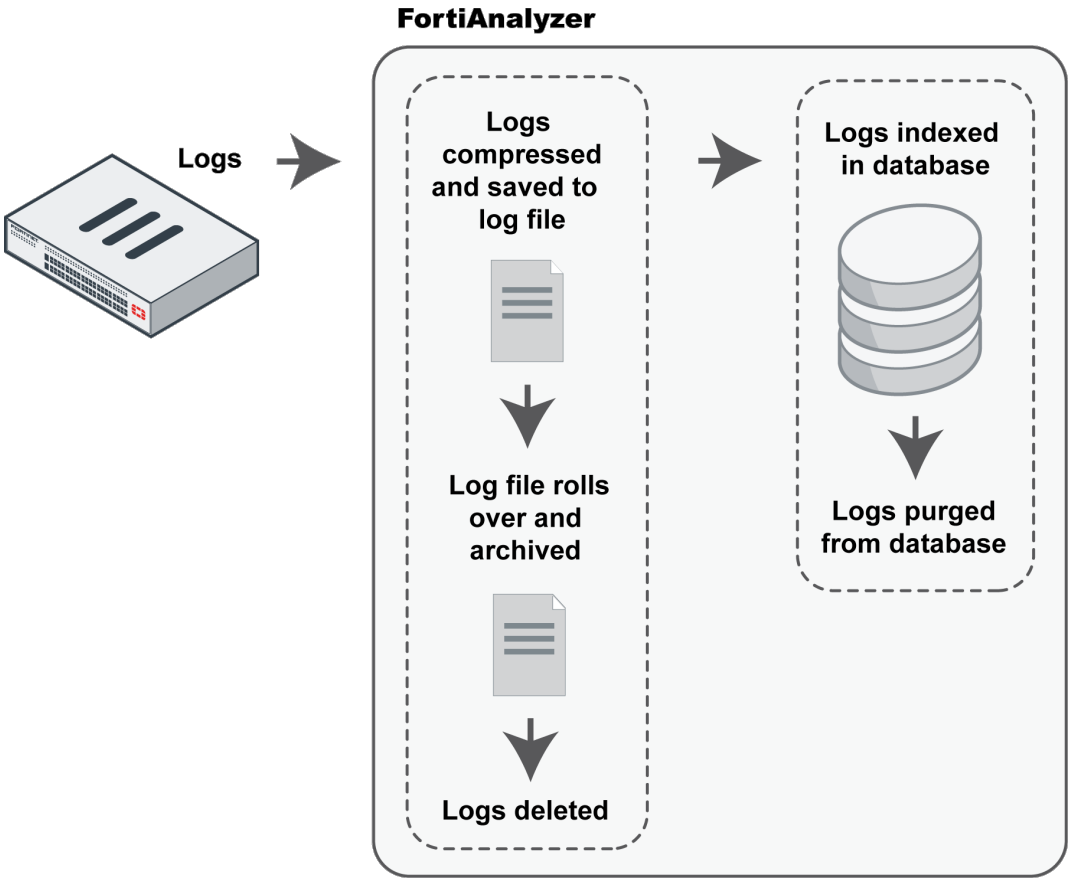
The following table summarizes the different automatic deletion polices:

| 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 Archive logs for the device are deleted. This policy affects only Archive 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 Archive logs are deleted for the device. This policy affects only Archive 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 archived 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 Archive logs and Analytics 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. Logs are available for analytic use in *FortiView*, *Event Monitor* and *Reports*. |
| Compressed | Compressed in log file | No. |

You can control how long to keep logs in indexed and compressed phases by using a data policy. See Configuring log storage policy on page 79.

# Configuring log storage policy

You can configure FortiAnalyzer log storage policy, which includes data policy and disk utilization settings.

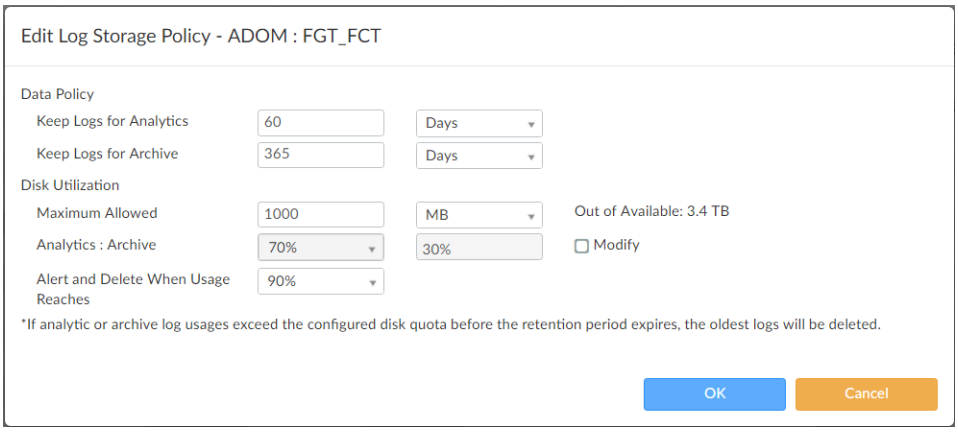
The log storage policy affects only the logs and SQL database of the device with which the log storage policy is associated. Reports are not affected. See FortiAnalyzer disk space allocation on page 75.

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

## Configuring log storage settings with ADOMs enabled

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

1. Go to *System Settings* > *Storage Info*.The page that opens presents an overview of the data policy and disk space usage of all ADOMs. See also Viewing log storage policy of all ADOMs on page 82
2. Select an ADOM, and click *Edit*. The *Edit ADOM Storage Configurations* dialog box is displayed.



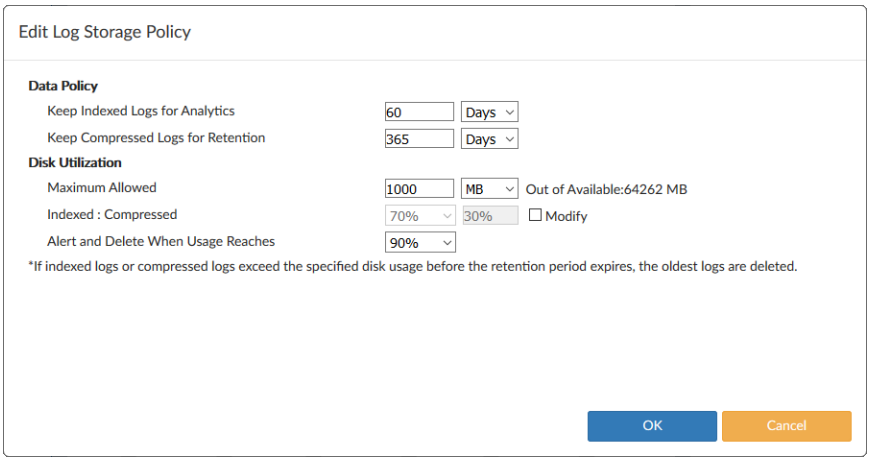

3. Configure the settings, and click *OK*.

| | | |
|---|---|---|
| **Data Policy** | | |
| | **Keep Logs for Analytics** | Specify how long to keep Analytics logs. |
| | **Keep Logs for Archive** | Specify how long to keep Archive logs. Make sure your setting meets your organization's regulatory requirements. |
| **Disk Utilization** | | |
| | **Maximum Allowed** | Specify the maximum disk space allotted to this ADOM. See also FortiAnalyzer disk space allocation on page 75. |
| | **Analytics : Archive** | Specify the disk space ratio between Analytics and Archive logs. Analytics logs require more space than Archive logs. The factory setting is 60% : 40%. Select the *Modify* check box to change the setting. |
| | **Alert and Delete When Usage Reaches** | Specify at what fullness you want alert messages to be generated and logs to be automatically deleted. The oldest Archive log files or Analytics database tables are deleted first. |

## Configuring log storage settings with ADOMs disabled

**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.




3. Configure the settings as you do when ADOMs are enabled (see Configuring log storage settings with ADOMs enabled on page 79), and click *OK*.

## Monitoring log storage policy

You can get an overview of the data policy and disk usage of all ADOMs. You can also view visualizations of the disk usage of a specific ADOM.

## Viewing log storage policy of all ADOMs

**To view log storage policy of all ADOMs:**

- Go to *System Settings* > *Storage Info*. The log storage policy of all ADOMs is displayed in tabular format.

| Column Heading | Description |
|---|---|
| **Name** | Displays the name of the ADOM. ADOMs are listed in two groups: *FortiGates and FortiCarriers* and *Other Device Types*. |
| **Analytics (Actual/Config Days)** | Displays the age in days of the oldest Analytics logs (Actual Days), as well as the number of days that Analytics logs will be kept according to the data policy (Config Days). |
| **Archive (Actual/Config Days)** | Displays the age in days of the oldest Archive logs (Actual Days), as well as the number of days that Archive logs will be kept according to the data policy (Config Days). |
| **Max Storage** | Displays the maximum disk space that is allotted for this ADOM (Analytics and Archive logs altogether). For more info about the maximum available space for each FortiAnalyzer unit, see FortiAnalyzer disk space allocation on page 75. |
| **Analytic Usage (Used/Max)** | Displays how much disk space that Analytics logs have used, as well as the maximum disk space allotted for Analytics logs. |
| **Archive Usage (Used/Max)** | Displays how much disk space that Archive logs have used, as well as the maximum disk space allotted for Archive logs. |

You can double-click an ADOM entry to configure its log storage settings. See Configuring log storage settings with ADOMs enabled on page 79.

## Viewing disk usage visualizations of each individual ADOM

**To view disk usage visualizations of each individual ADOM:**

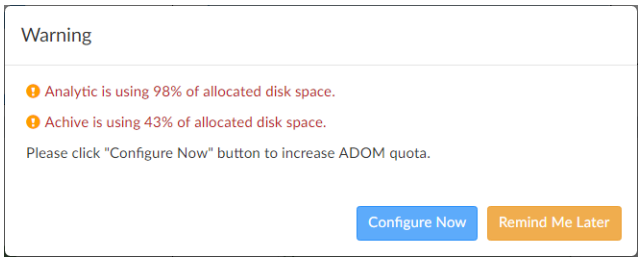
- Go to *Log View* > *Storage Statistics*. Visualizations of disk space usage of both Analytics and Archive logs are displayed, with Analytic Policy charts showing an overview, and Analytic Details charts showing the disk space usage details.

You can also access *Storage Statistics* from *Device Manager* > *Storage Used*.

- Hover the mouse over the charts to view more information about the chart or data point.
- For the Analytic Details and Archive Details line charts, you can click on a data point to drill down into a breakdown by device.

| Charts | Description |
|---|---|
| **Analytic Policy** | Displays how much of the disk quota for Analytics logs has been used, as well as the Actual and Configure Days of the Analytics logs. |
| **Analytic Details** | Shows the disk usage by Analytics logs over time. The blue line shows actual usage, and the red horizontal line marks the maximum allotted disk space. Double click a data point to drill down into a breakdown by device. |
| **Archive Policy** | Displays how much of the disk quota for Archive logs has been used; as well as the Actual and Configure Days of the Archive logs. |
| **Archive Details** | Shows the disk usage by Archive logs over time. The blue line shows actual usage, and the red horizontal line marks the maximum allotted disk space. Double click a data point to drill down into a breakdown by device. |

When the ADOM is reaching its maximum disk quota, a warning dialog box will be displayed. If you click *Configure Now*, it will direct you to the Edit Log Storage Policy dialog box to adjust log storage policy. See Configuring log storage settings with ADOMs enabled on page 79.




# Configuring global log and file settings

## Configuring global automatic deletion

FortiAnalyzer allows you to configure automatic deletion of Archive 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 76 and Data policy and automatic deletion on page 20.

**To configure global automatic deletion settings:**

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

| | |
|---|---|
| **Device log files older than** | 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 (*Hours*, *Days*, *Weeks*, or *Months*). See also Archive logs and Analytics logs on page 20. |

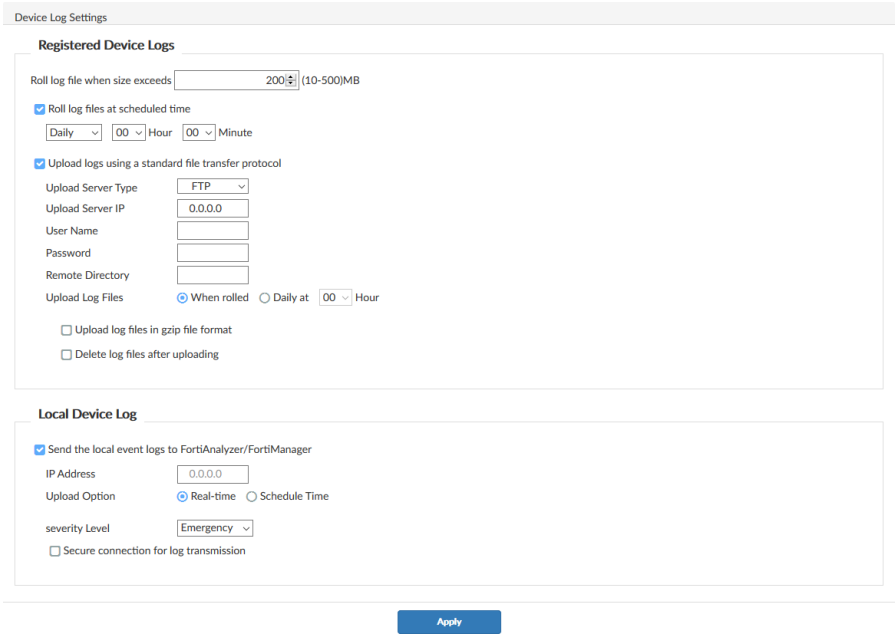
| | |
|---|---|
| **Quarantined files older than** | Select to enable automatic deletion of quarantined, compressed log files. Enter a value in the text field, and select the time period from the drop-down list. |
| **Reports older than** | Select to enable automatic deletion of reports of data from compressed log files. Enter a value in the text field, and select the time period from the drop-down list. |
| **Content archive files older than** | Select to enable automatic deletion of IPS and DP archives from Archive 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.




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

| **Registered Device Logs** | |
|---|---|
| **Roll log file when size exceeds** | Enter the log file size. Range: 10 to 500 MB |

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

## 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 84. 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. |

# 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.

In 5.4.1, *FortiView* is supported for FortiGate, FortiCarrier, and FortiClient EMS devices.

### 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 Analytics logs. Data from Archive logs is not displayed in *FortiView*. For more information, see Archive logs and Analytics logs on page 20.

### FortiView summary list and description

#### FortiView summaries for FortiGate and FortiCarrier devices

| Category | View | Description |
|---|---|---|
| **Summary** | An overview | An overview of most used *FortiView* summary views |
| **Threats** | 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:<br>• Risk applications detected by application control<br>• Intrusion incidents detected by IPS<br>• Malicious web sites detected by web filtering<br>• Malware/botnets detected by antivirus.<br>**Note**: If you are running FortiOS 5.0.x, you must enable Client Reputation in the security profiles on the FortiGate in order to view entries in Top Threats. |
| | 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 Viewing the threat map on page 95. |

| Category | View | Description |
|---|---|---|
| | Indicators of Compromise | Displays end users with suspicious web use compromises, including end users' IP addresses, overall threat rating, and number of threats. Drill-downs are available to view threat details.<br>**Note**: To use this feature, 1) UTM logs of the connected FortiGate devices must be enabled; 2) The FortiAnalyzer needs to subscribe to FortiGuard to keep its threat database up to date. |
| **Traffic** | 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 traffic information about top countries in terms of traffic sessions, including application, threat, source and destination. |
| | 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 |
| **Application & Websites** | 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. |
| **VPN** | 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 |
|---|---|---|
| **WiFi** | 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 |
| **System** | 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 |
| | Failed Authentication Attempts | Displays the IP addresses of the users who failed to log into the managed device |
| **Endpoints** | All Endpoints | Lists the FortiClient endpoints that are registered to the FortiGate device. |
| | Endpoints Vulnerabilities | Displays vulnerability information about the FortiClient endpoints that are registered to the FortiGate device, such as vulnerability name, category, CVE information, severity, FortiGuard link, and remediation action. |

## FortiView summaries for FortiClient EMS devices

| Category | View | Description |
|---|---|---|
| **Threats** | 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:<br>• Risk applications detected by application control<br>• Malicious web sites detected by web filtering<br>• Malware/botnets detected by antivirus. |
| **Application & Websites** | Top Applications | Displays information about the top applications being used on the network, including the application name, category, and risk level |
| | Top Websites | Displays the top allowed and blocked web sites on the network |

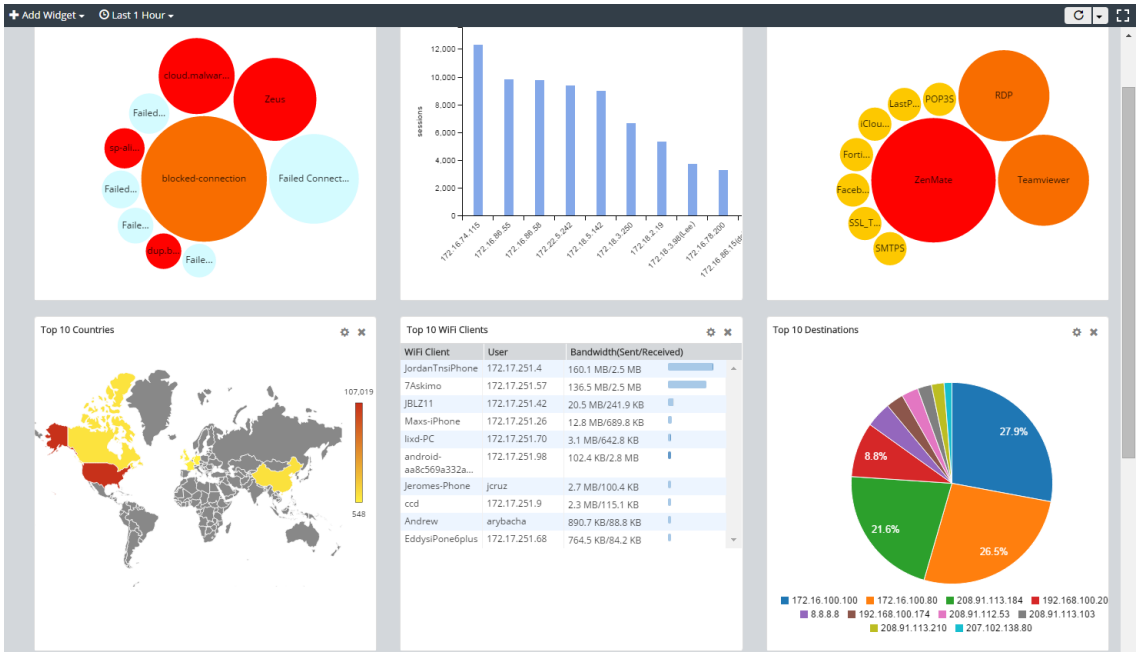
| Category | View | Description |
|---|---|---|
| **Endpoints** | All Endpoints | Lists the FortiClient endpoints that are registered to the FortiClient EMS device. |
| | Endpoints Vulnerabilities | Displays vulnerability information about the FortiClient endpoints that are registered to the FortiClient EMS device, such as vulnerability name, category, CVE information, severity, FortiGuard link, and remediation action. |

# 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 25.

## 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.

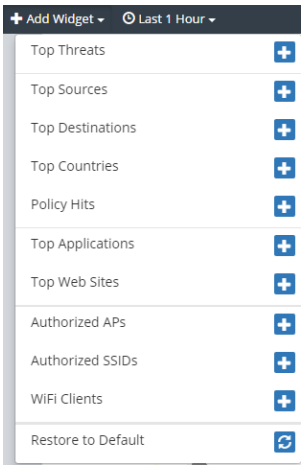



You can create multiple views/widgets for a FortiView summary. For example, you can create two Top Threats views: one of Top 10 Threats view in bubble chart format, and one of Top 20 Threats in table format.

## 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.

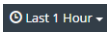



You can now see the newly added widget on the *Summary* page.

**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 period* drop-down list 

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.

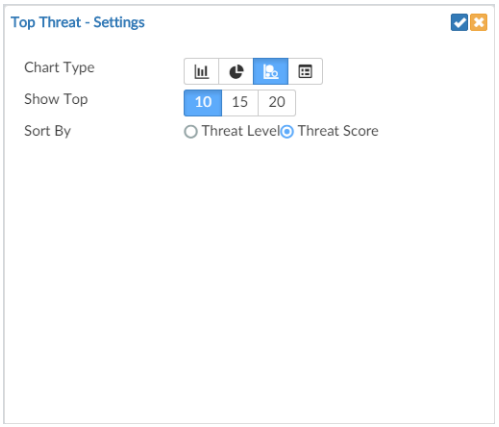
## Viewing each widget on the Summary page

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 93.

### Configuring the view settings for an individual widget:

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

1. 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.




2. On the settings panel, configure the settings for the widget, such as *Chart Type*, *Show Top,* and *Sort By*.
3. 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.

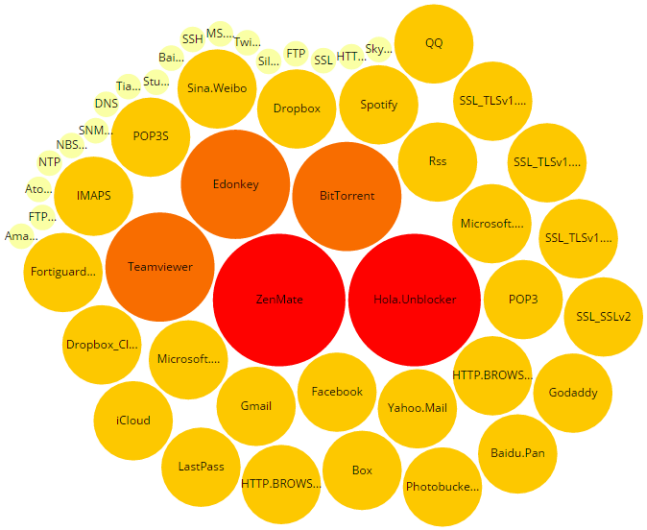
**To view summary information in tabular format:**

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.



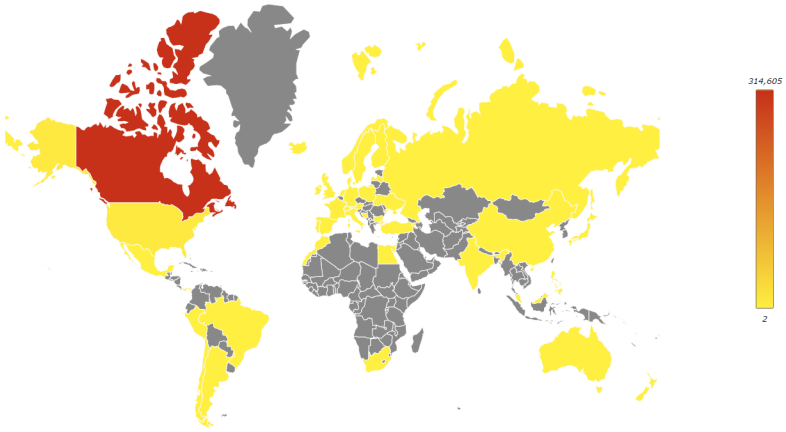

4. Choose a sort method for the graphic from the *Sort By* list in the top-right corner.
5. Hover the mouse over a graphical element to view more information.
6. Click an element to drill down. You can then view details about different dimensions of the entry in different tabs.
7. You can continue drilling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

## 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.

## 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 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 filtered summaries to PDF

You can export to PDF filtered FortiView summaries or any level of the drilldowns.

**To export filtered summaries to PDF:**

1. In the filtered summary view or its drilldown, click *Export to PDF* in the top-right corner.
2. In the *Export to PDF* dialog box that opens, review and configure the settings:
   - Type a PDF file name.
   - From the *Top* drop-down list, specify the number of entries to export.
   - (If you are in a drilldown view) In the *Drilldown* section, the tab that you are in is selected by default. You can select more tabs if you want.
3. Click *OK*.

**Note**: The filtered summaries will be exported in the tabular format, no matter in which format (tabular or graphical) you execute the export function.

## Exporting filtered summaries to report charts

You can export filtered FortiView summaries of any level of the drilldowns to report charts.

**Note**: Only the log field filters are exported. The device and time period filters are not exported.

**To export filtered summaries to report charts:**

1. In the filtered summary view or its drilldown, click *Export to Report Chart* in the top-right corner.
2. In the *Export to Report Chart* dialog box that opens, review and configure the settings:
   - Type a chart name.
   - From the *Show Top* drop-down list, specify the number of entries to export.
   - (If you are in a drilldown view) In the *Drilldown* section, the tab that you are in is selected by default. You can select more tabs if you want. One chart will be created for each tab.
3. Click *OK*.

The charts are saved in the Chart Library. You can use them in the same way as you use other charts.

**Note**: The filtered summaries will be exported in the tabular format, no matter in which format (tabular or graphical) you execute the export function.

## Viewing end users' Indicators of Compromise (IOC) information

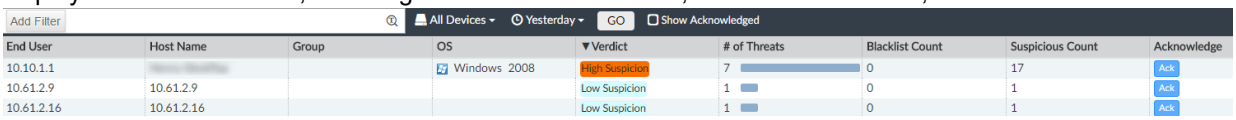
The *Indicators of Compromise* summary shows end users with suspicious web usage compromises. It provides information such as end users' IP addresses, overall threat rating, and number of threats. Drill-downs are available to view threat details.

To generate this IOC summary view, the FortiAnalyzer unit checks the web filter logs of each end user against its threat database. When a threat match is found, a threat score is given to the end user. When the check is completed, FortiAnalyzer will aggregate all the threat scores of an end user and give its verdict on the overall IOC of the end user.

To use this IOC summary, you must turn on the UTM web filter of FortiGate devices. You must also subscribe your FortiAnalyzer unit to FortiGuard to keep its local threat database synced with the FortiGuard threat database. See Subscribing FortiAnalyzer to FortiGuard on page 97.

**To view end users' IOC information:**

1. Go to *FortiView* > *Threats* > *IOC*. In the content pane, an overview of end users with suspicious compromises is displayed in tabular format, including end users' IP addresses, overall threat verdict, and number of threats.




2. You can filter the entries by adding filters, as well as specifying devices or a time period.
3. You can acknowledge the IOC of an end user by clicking *Ack* in the Acknowledge column.
4. You can double-click an entry to drill down and view threat details.

### Subscribing FortiAnalyzer to FortiGuard

Your FortiAnalyzer needs to subscribe to FortiGuard to keep its threat database up to date. You need to purchase a FortiGuard IOC Service license for that.

**To subscribe your FortiAnalyzer to FortiGuard:**

1. Go to *System Settings* > *Dashboard*.
2. In the *License Information* widget, find the *FortiGuard* > *IOC Service* field and click *Purchase*.

## Monitoring resource usage of devices

You can monitor how much FortiAnalyzer system resources (e.g., CPU, memory, and disk space) that each device uses. When ADOMs are enabled, this information is displayed per ADOM. In a specific ADOM, you can view the resource usage information of all the devices under the ADOM.

**To monitor resource usage for devices:**

- Go to *FortiView* > *System* > *Resource Usage*.

# 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 already 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 group.

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 Analytics logs and Archive logs:

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

For more information, see Archive logs and Analytics logs on page 20.

### 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 |
| **FortiGate** | Traffic<br>Event: Compliance Events, Endpoint, HA, System, Router, VPN, User, WAN Opt. & Cache, and Wireless<br>Security: Vulnerability Scan, Antivirus, Web Filter, Application Control, Intrusion Prevention, Email Filter, Data Leak Prevention, Web Application Firewall<br>FortiClient<br>VoIP<br>Content logs are also collected for FortiOS 4.3 devices. |
| **FortiCarrier** | Traffic, Event, GTP |
| **FortiCache** | Traffic, Event, Antivirus, Web Filter |

| Device Type | Log Type |
|---|---|
| **FortiClient** | Traffic, Event, Vulnerability Scan |
| **FortiDDoS** | Event, Intrusion Prevention |
| **FortiMail** | History, Event, Antivirus, Email Filter |
| **FortiManager** | Event |
| **FortiSandbox** | Malware, Network Alerts |
| **FortiWeb** | Event, Intrusion Prevention, Traffic |
| **Syslog** | 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 group.

## 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 25.

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

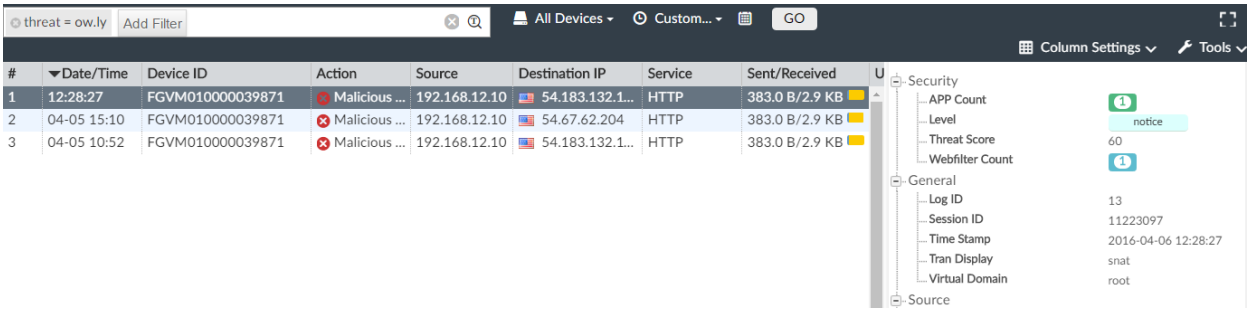
**To view the log message list:**

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.

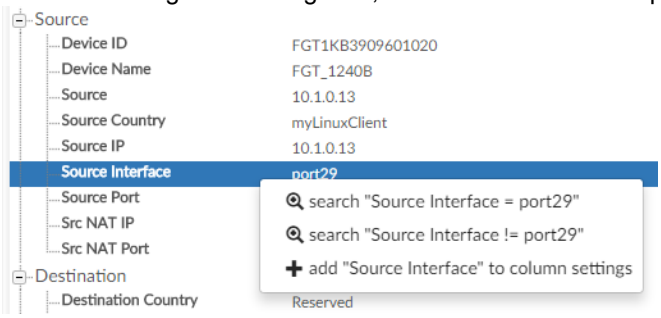
## Viewing log message details

**To view log message details:**

- Double-click a log message on the log message list. The log details pane is displayed to the right side of the log message list, with the log fields categorized in tree view.
- (Alternative) Select the log message and then click *Display Details* in the bottom right corner.

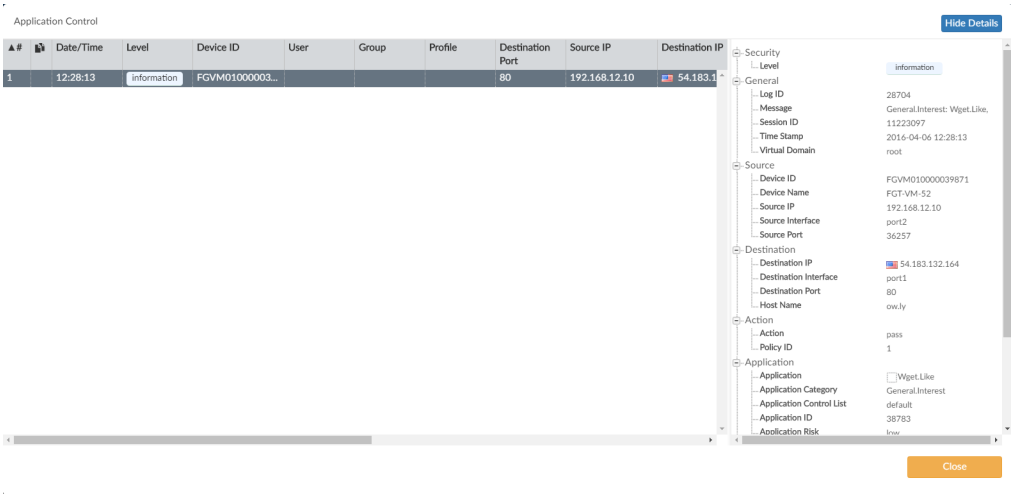



Log details pane also provides shortcuts for adding filters as well as showing or hiding a column. Just right-click a log field, and select the desired option.



**To view UTM logs:**

- If the log message contains UTM logs, you can click the UTM log icon in the log details pane to open the UTM log view window.




## 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.
   **Note**: 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.

You can also add or remove a log field column in the log details pane, by right-clicking a log field and selecting *Add* [*log field name*] or *Remove* [*log field name*].

**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 messages by using the filters in the toolbar or by using a context-sensitive filter of a log message.

**To filter log messages by using the filters in the toolbar:**

1. Specify search criteria in the search bar.
   - Use Regular Search. In the selected log view, click in the *Add Filter* box, select a filter from the drop-down list, and type a value. You can use operators such as OR, NOT, Greater than, and Less than. See also Search operators and syntax on page 104.
     **Note**: Only columns that are displayed are available on the drop-down filter list.
   - Use Advanced Search. Click the *Switch to Advanced Search* icon at the end of the search bar. In the Advanced Search mode, you type the search criteria (log field names and their values). You can click next to the search bar to open the Search operators and syntax pane (which is also described in Search operators and syntax on page 104). You can click *Switch to Regular Search* icon to go back to regular search.
   - You can also type any string in the search bar to start a “freestyle" search. FortiAnalyzer will then search the string within the indexed fields that can be configured using the CLI command: `config ts-index-field`. For example, if the indexed fields have been configured like this using the CLI command:

     ```
     config system sql
     config ts-index-field
     edit "FGT-traffic"
     set value "app,dstip,proto,service,srcip,user,utmaction"
     next
     end
     end
     ```

     Then if you type "`Skype`" in the search bar, FortiAnalyzer will search for “Skype” within these indexed fields: *app,dstip,proto,service,srcip,user*, and *utmaction*.

     You can combine freestyle search with other search methods, for example, “`Skype user=David`”.

The filters are case-insensitive by default. If you want to make your filters case-sensitive, select *Case Sensitive Search* from the *Tools* drop-down menu in the tool bar.

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 a context-sensitive filter :**

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

  Depending on the column in which your cursor is placed 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.

You can get the corresponding log field name of a filter/column name by right-clicking on the column of any log entry and selecting a context-sensitive filter. The filter will be displayed in the search bar, with the filter name translated into the corresponding log field name.

The context-sensitive filters are also available for each log field in the log details pane. See Viewing log message details on page 101.

### Search operators and syntax

| Operators or symbols | Syntax |
|---|---|
| **And** | Find log entries that contain all the search terms. Connect the terms with a space character, or “and”.<br>Example: `user=henry group=sales`; (alternative) `user=henry and group=sales` |
| **Or** | Find log entries that contain any of the search terms. Separate the terms with “or” or a comma “,”.<br>Examples: 1) `user=henry or srcip=10.1.0.15`; 2) `user=henry,linda` |
| **Not** | Find log entries that do NOT contain the search terms. Add “-” before the field name.<br>Example: `-user=henry` |
| **>, <** | Find log entries greater than or less than a value, or within a range. Can only be applied to Integer field type.<br>Example: `policyid>1 and policyid<10` |
| **IP subnet/range search** | You can search for log entries within a certain IP subnet or range.<br>Examples: 1) `srcip=192.168.1.0/24`; 2) `srcip=10.1.0.1-10.1.0.254` |
| **Wildcard search** | You can use wildcard searches for all field types.<br>Examples: 1) `srcip=192.168.1.*`; 2) `policyid=1*`; 3) `user=*` |

### 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 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.

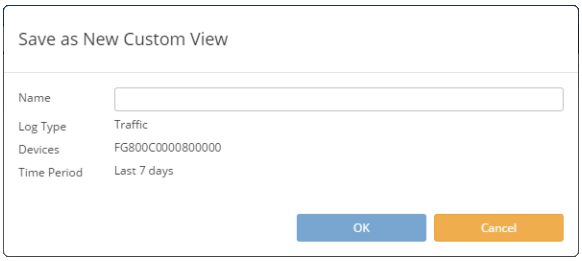
For more information about FortiGate raw logs, see the *FortiGate Log Message Reference* in the Fortinet Document Library. For more information about raw logs of other devices, see the *Log Message Reference* for the platform type.

## 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:**

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 content pane, customize the log view as you want, for example, by adding filters, specifying devices, or specifying a time period.
4. Select *Custom View* from *Tools* in the tool bar. The *Create New Custom View* dialog box opens.




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 108. You can preview the chart in the *Preview* box.
5. Click *Save*.

For more information about creating charts, see Chart library on page 131

# Log groups

You can group devices into log groups. You can then specify to view FortiView summaries, display logs, generate reports, or create handlers for a log group, as you can specify to perform such activities for an individual device. Log groups are virtual. They do not have SQL databases or occupy additional disk space.

In FortiAnalyzer 5.0.6 and earlier, log groups can be treated as a single device which has its own SQL database. This has been changed since FortiAnalyzer 5.2.

## Creating log groups

**To create a new log group:**

1. Go to *Log View* > *Log Group*.
2. In the content pane, click *Create New* in the toolbar.
3. In the *Create New Log Group* dialog box that opens, type a log group name and add devices to the log group.
4. Click *OK*.The newly created log group is shown on the log group list.

When you add a device with VDOMs to a log group, all VDOMs are automatically added.

# Log Browse

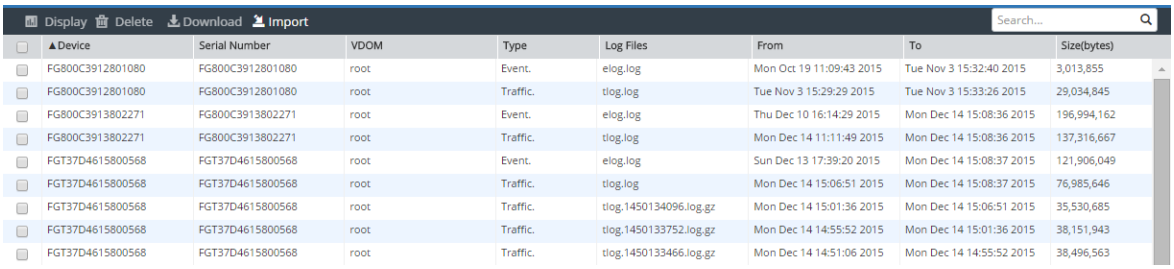
When a log file reaches its maximum size or a scheduled time, the FortiAnalyzer rolls the active log file by renaming the file. The file name will be in the form of `xlog.N.log`, where `x` is a letter indicating the log type, and `N` is a unique number corresponding to the time the first log entry was 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 101.




| Device | Serial Number | VDOM | Type | Log Files | From | To | Size(bytes) |
|---|---|---|---|---|---|---|---|
| FG800C3912801080 | FG800C3912801080 | root | Event. | elog.log | Mon Oct 19 11:09:43 2015 | Tue Nov 3 15:32:40 2015 | 3,013,855 |
| FG800C3912801080 | FG800C3912801080 | root | Traffic. | tlog.log | Tue Nov 3 15:29:29 2015 | Tue Nov 3 15:33:26 2015 | 29,034,845 |
| FG800C3913802271 | FG800C3913802271 | root | Event. | elog.log | Thu Dec 10 16:14:29 2015 | Mon Dec 14 15:08:36 2015 | 196,994,162 |
| FG800C3913802271 | FG800C3913802271 | root | Traffic. | tlog.log | Mon Dec 14 11:11:49 2015 | Mon Dec 14 15:08:36 2015 | 137,316,667 |
| FGT37D4615800568 | FGT37D4615800568 | root | Event. | elog.log | Sun Dec 13 17:39:20 2015 | Mon Dec 14 15:08:37 2015 | 121,906,049 |
| FGT37D4615800568 | FGT37D4615800568 | root | Traffic. | tlog.log | Mon Dec 14 15:06:51 2015 | Mon Dec 14 15:08:37 2015 | 76,985,646 |
| FGT37D4615800568 | FGT37D4615800568 | root | Traffic. | tlog.1450134096.log.gz | Mon Dec 14 15:01:36 2015 | Mon Dec 14 15:06:51 2015 | 35,530,685 |
| FGT37D4615800568 | FGT37D4615800568 | root | Traffic. | tlog.1450133752.log.gz | Mon Dec 14 14:55:52 2015 | Mon Dec 14 15:01:36 2015 | 38,151,943 |
| FGT37D4615800568 | FGT37D4615800568 | root | Traffic. | tlog.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.

### 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 |
|---|---|
| **Name** | Type a name for the chart. |

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

# 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 25.

### 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.

**Note**: FortiAnalyzer 5.4 provides predefined event handlers for FortiGate and FortiCarrier devices. For other devices, you will have to create your own event handlers.

### Logs used for events

*Event Monitor* displays events from Analytics logs. Archive logs are not used to generate events. For more information, see Archive logs and Analytics 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.

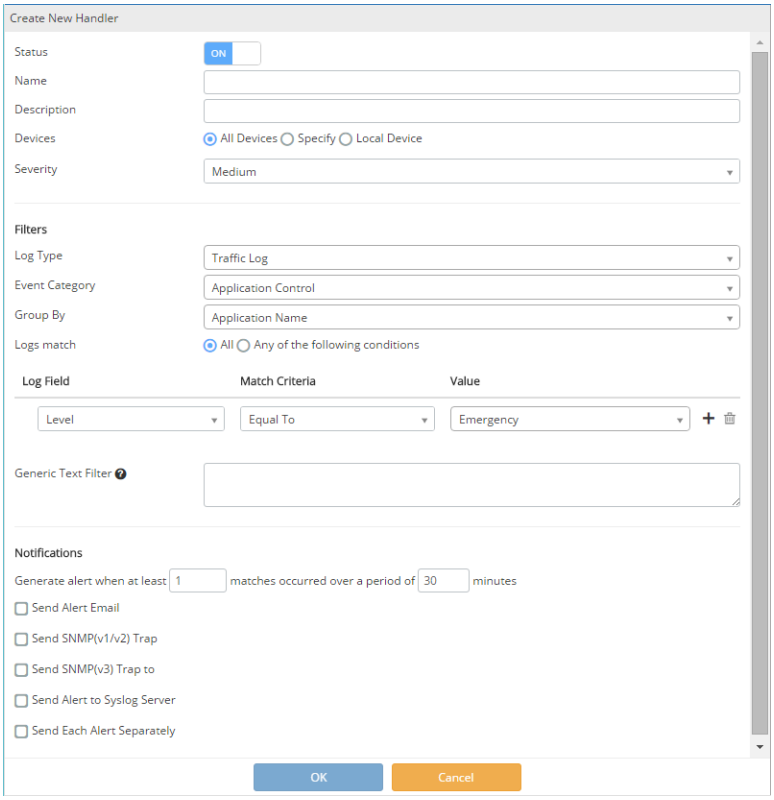
**To enable event handlers:**

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 118.



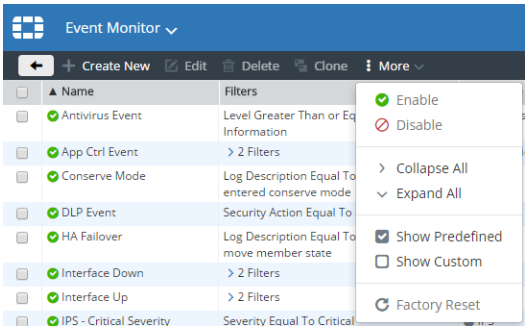
6. Click *OK*.

## 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

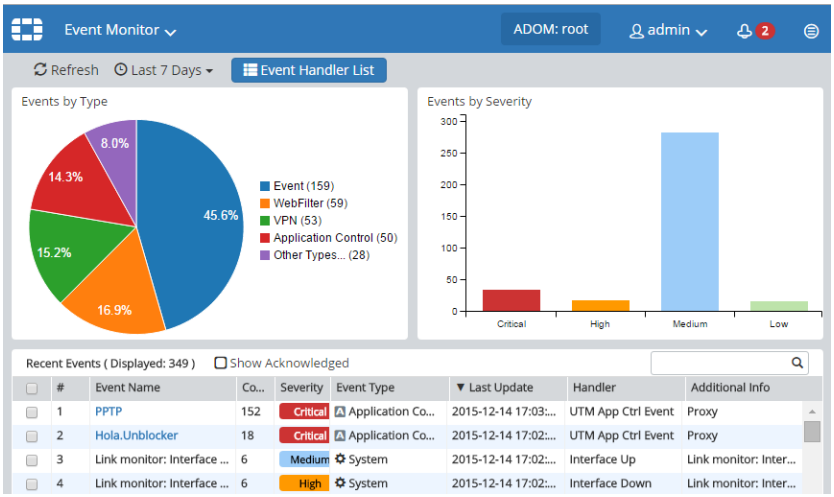
You can manage event handler by going to *Event Monitor* > *Event Handler List*. The following table shows the options available.

| Option | Description |
|---|---|
| **Create New** | Create a new event handler. This option is available in the toolbar and right-click menu. |
| **Edit** | Edit the selected event handler. |
| **Delete** | Delete the selected event handler. You cannot delete predefined event handlers. |
| **Clone** | Clone the selected event handler. A cloned entry will have *Copy* added to its name field. You can rename the cloned entry while editing the event handler. |
| **Enable** | Enable the selected event handler to start generating events on the *Event Management* > *All Events* page. |
| **Disable** | Disable the selected event handler to stop generating events on the *Event Management* > *All Events* page. |
| **Factory Reset** | 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 114.
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.

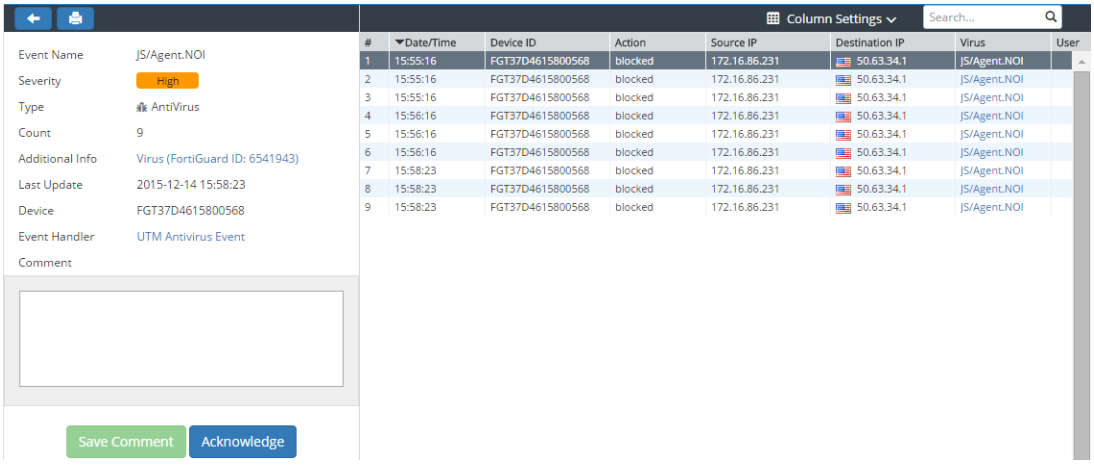
   You can view event details by double-clicking an event summary entry. See Viewing event details on page 114.

## 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.

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




## Acknowledging events

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

**To acknowledge event(s):**

1. From the event list, select one or multiple events that you would like to acknowledge.
2. 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<br>Log Type: Traffic Log<br>Event Category: Antivirus<br>Group by: Virus Name<br>Log messages that match all conditions:<br>• *Level Greater Than or Equal To Information* |

| Event Handler | Description |
|---|---|
| App CTRL Event | Severity: Medium<br>Log Type: Traffic Log<br>Event Category: Application ControlGroup by: Application Name<br>Log messages that match any of the following conditions:<br>• *Application Category Equal To Botnet*<br>• *Application Category Equal To Proxy* |
| Conserve Mode | Severity: Critical<br>Log Type: Event Log<br>Event Category: System<br>Group by: Message<br>Log messages that match all conditions:<br>• *Log Description Equal To System services entered conserve mode* |
| DLP Event | Severity: Medium<br>Log Type: Traffic Log<br>Event Category: DLP<br>Group by: DLP Rule Name<br>Log messages that match all conditions:<br>• *Security Action Equal To Blocked* |
| HA Failover | Severity: Medium<br>Log Type: Event Log<br>Event Category: HA<br>Group by: Log Description<br>Log messages that match all conditions:<br>• *Log Description Equal To Virtual cluster move member* |
| Interface Down | Severity: High<br>Log Type: Event Log<br>Event Category: System<br>Group by: Message<br>Log messages that match all conditions:<br>• *Action Equal To interface-stat-change*<br>• *Status Equal To DOWN* |
| Interface Up | Severity: Medium<br>Log Type: Event Log<br>Event Category: System<br>Group by: Message<br>Log messages that match all conditions:<br>• *Action Equal To interface-stat-change*<br>• *Status Equal To UP* |

| Event Handler | Description |
|---|---|
| IPS - Critical Severity | Severity: Critical<br>Log Type: IPS<br>Group by: Attack Name<br>Log messages that match all conditions:<br>• *Severity Equal To Critical* |
| IPS - High Severity | Severity: High<br>Log Type: IPS<br>Group by: Attack Name<br>Log messages that match all conditions:<br>• *Severity Equal To High* |
| IPS - Medium Severity | Severity: Medium<br>Log Type: IPS<br>Group by: Attack Name<br>Log messages that match all conditions:<br>• *Severity Equal To Medium* |
| IPS - Low Severity | Severity: Low<br>Log Type: IPS<br>Group by: Attack Name<br>Log messages that match all conditions:<br>• *Severity Equal To Low* |
| IPsec Phase2 Down | Severity: Medium<br>Log Type: Event Log<br>Event Category: VPN<br>Group By: VPN Tunnel<br>Log messages that match all conditions:<br>• *Action Equal To phase2-down* |
| IPsec Phase2 Up | Severity: Medium<br>Log Type: Event Log<br>Event Category: VPN<br>Group By: VPN Tunnel Log messages that match all conditions:<br>• *Action Equal To phase2-up* |
| Local Device Event | Devices: Local FortiAnalyzerSeverity: Medium<br>Log Type: Event Log<br>Event Category: Endpoint<br>Log messages that match all conditions:<br>• *Level Greater Than or Equal To Warning* |

| Event Handler | Description |
|---|---|
| Power Supply Failure | Severity: Critical<br>Log Type: Event Log<br>Event Category: System<br>Group by: Message<br>Log messages that match any of the following conditions:<br>• *Action Equal To power-supply-monitor*<br>• *Status Equal To failure* |
| UTM Antivirus Event | Severity: High<br>Log Type: Virus<br>Group by: Virus Name<br>Log messages that match all conditions:<br>• *Level Greater Than or Equal To Information* |
| UTM App CTRL Event | Severity: Medium<br>Log Type: Application Control<br>Group by: Application Name<br>Log messages that match any of the following conditions:<br>• *Application Category Equal To Botnet*<br>• *Application Category Equal To Proxy* |
| UTM DLP Event | Severity: Medium<br>Log Type: DLP<br>Group by: DLP Rule Name<br>Log messages that match all conditions:<br>• *Action Equal To Block* |
| UTM Web Filter Event | Severity: Medium<br>Log Type: Web Filter<br>Group by: Category<br>Log messages that match any of the following conditions:<br>• *Web Category Equal To Child Abuse*, *Discrimination*, *Drug Abuse*, *Explicit Violence*, *Extremist Groups*, *Hacking*, *Illegal or Unethical*, *Plagiarism*, *Proxy Avoidance*, *Malicious Websites*, *Phishing*, *Spam URLs* |
| Web Filter Event | Severity: Medium<br>Log Type: Traffic Log<br>Event Category: WebFilter<br>Group by: Category<br>Log messages that match any of the following conditions:<br>• *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* |

## Create New Handler pane

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

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

| Field | Description |
|---|---|
| **Generate alert when at least** | Enter threshold values to generate alerts. Enter the number, in the first text box, of each type of event that can occur in the number of minutes entered in the second text box. |
| **Send Alert Email** | Select the checkbox to enable. Enter an email address in the *To* and *From* text fields, enter a subject in the *Subject* field, and select the email server from the drop-down list. Select the add icon to add an email server. For information on creating a new mail server, see Mail servers on page 182. |
| **Send SNMP(...) Trap to** | 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. |
| **Send Alert to Syslog Server** | Select the checkbox to enable this feature. Select a syslog server from the drop-down list. Select the add icon to add a syslog server. For information on creating a new syslog server, see Syslog servers on page 183 |
| **Send Each Alert Separately** | Select to send each alert individually, instead of in a groups. |

# 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 76.

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 25.

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 | *Reports* > *Report Definitions* > *All Reports* | 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 | *Reports* > *Report Definitions* > *Templates* | 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 *Layout* tab of a report that is to be created. See List of report templates on page 142. |

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

## Logs used for reports

*Reports* uses Analytics logs to generate reports. Archive logs are not used to generate reports. For more information, see Data policy and automatic deletion on page 20.

## 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 hcaches. 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 144 and Creating charts on page 131 and Creating macros on page 135.
4. In the toolbar of the *View Report* tab, click *Run Report*.

## Viewing completed reports

After you generate reports, you can view competed 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 122.

**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*.

## Grouping reports

If you are running a large number of reports which are very similar, you can significantly improve report generation time by grouping the reports. Report grouping can reduce the number of hcache tables and improve auto-hcache completion time and report completion time.

### Step 1: Configure report grouping

To group reports with titles containing string `Security_Report` by device ID and VDOM, enter the following CLI commands:

```
config system report group
   edit 0
      set adom root
      config group-by
         edit devid
         next
         edit vd
         next
   end
   set report-like Security_Report
   next
end
```

Notes:

1. The `report-like` field is the name pattern of the report that will utilize the `report-group` feature. This string is case-sensitive.
2. The `group-by` value controls how cache tables are grouped.
3. To see a list of reports that have been included in the grouping, enter the following CLI command:

   ```
   execute sql-report list-schedule <ADOM>
   ```

### Step 2: Initiate a rebuild of hcache tables

To initiate a rebuild of hcache tables, enter the following CLI command:

```
diagnose sql rebuild-report-hcache <start-time> <end-time>
```

Where `<start-time>` and `<end-time>` are in the format: `<yyyy-mm-dd hh:mm:ss>`.

## Retrieving report generation logs

Once you start running a report, a log about the report generation status and system performance is created. You can use this log to troubleshoot report generation problems and tune the system. For example, if your report is very slow to generate, you can check this log to find out which charts cost the longest time to generate and the system performance.

**To retrieve report generation logs:**

1. After you run a report (see Generating reports on page 123), find the report that is being or has been generated in the *View Report* tab.
2. Right-click the report, and select *Retrieve Diagnostic*.
3. Save the log to your computer, and then open it in a text editor.

## 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.
   **Note**: The following characters are NOT supported in report names:
   \ / " ' < > & , | # ? % $ +
   b. Select *From Template* for the *Create from* setting, and select a template from the drop-down list. The template populates the *Layout* tab of the report.
5. On the *Settings* tab, configure the settings. For a description of the fields, see Reports Settings tab on page 144.
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 146.
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.
   **Note**: The following characters are NOT supported in report names:
   \ / " ' < > & , | # ? % $ +

5. Edit settings on the *Settings* tab. For a description of the fields, see Reports Settings tab on page 144.
6. Editing settings on the *Layout* tab.
   For a description of the fields, see Reports Layouts tab on page 146.
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.
      **Note**: The following characters are NOT supported in report names:
      \ / " ' < > & , | # ? % $ +
   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 144.

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 146. For information about creating charts and macros, see Creating charts on page 131 and Creating macros on page 135.
7. Click *OK*.

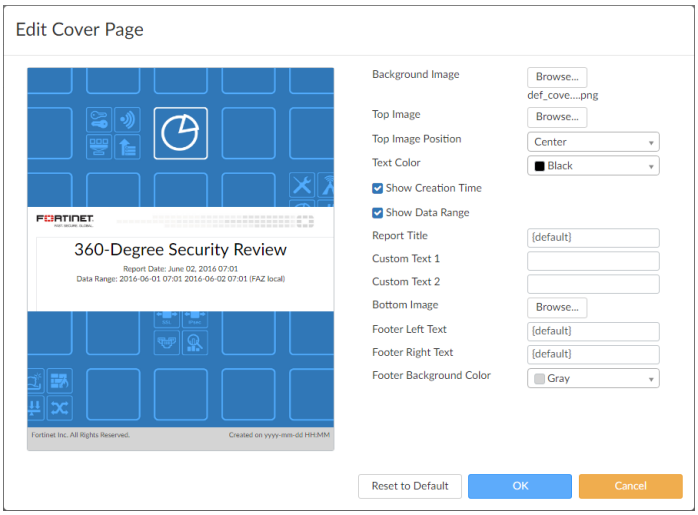
## Customizing report cover pages

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 a report cover page:**

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. Go to the *Advanced Settings* section in the *Settings* tab, select the *Print Cover Page* check box, and click *Customize* next to the check box. The *Edit Cover Page* pane opens.




5. Configure the following settings:

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

| | |
|---|---|
| **Footer Right Text** | Edit the text printed in the left hand footer of the cover page. `{default}` prints the report creation date and time. |
| **Footer Background Color** | Select the cover page footer background color from the drop-down list. Select one of the following: *Bold Blue*, *Blue*, *Turquoise*, *Green*, *Bold Green*, *Yellow*, *Orange*, *Red*, *Bold Red*, *Purple*, *White*, *Gray*, *Transparent*. |
| **Reset to Default** | 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 |
|---|---|
| **Create New** | Creates a new report. You can choose whether to base the new report on a report template. |
| **Edit** | Edits the selected report. |
| **Delete** | Deletes the selected report. |
| **Clone** | Clones the selected report. |
| **Run report** | Generates a report. |
| **Folder** | Organize reports into folders. |
| **Import Report** | Imports a report from a management computer. |
| **Export Report** | 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 Analytics 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 146. For information about creating charts and macros, see Creating charts on page 131 and Creating macros on page 135.

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 |
|---|---|
| **Create New** | Create a new report template |
| **Edit** | Edit a report template. You can edit report templates that you created. You cannot edit predefined report templates. |

| Option | Description |
|---|---|
| **View** | 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. |
| **Delete** | Deletes the selected report template. You can delete report templates that you created. You cannot delete predefined report templates. |
| **Clone** | Clones the selected report template |
| **Rename** | Renames the selected report template. You can rename report templates that you created. You cannot rename predefined report templates. |

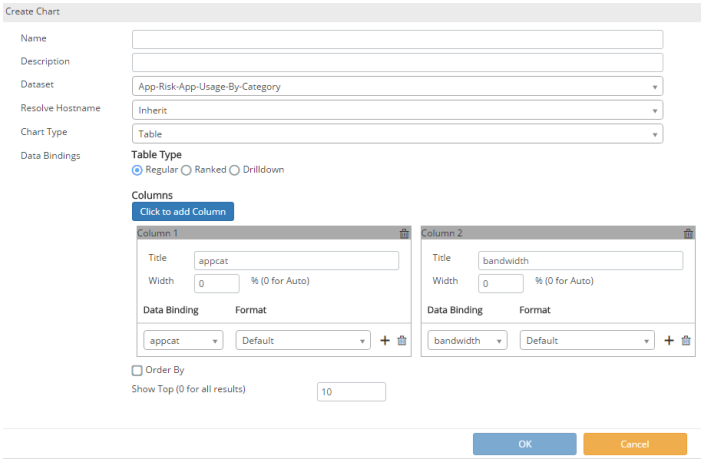
# Chart library

## 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 106.

**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.




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

| | |
|---|---|
| **Name** | Enter a name for the chart. |

| | | |
|---|---|---|
| **Description** | | Enter a description of the chart. |
| **Dataset** | | Select a dataset from the drop-down list. See Datasets on page 136 for more information. The options will vary based on device type. |
| **Resolve Hostname** | | Select to resolve the hostname. Select one of the following: *Inherit*, *Enabled*, or *Disabled*. |
| **Chart Type** | | Select a graph type from the drop-down list; one of: area, *bar*, *donut*, *line*, *pie*, or *table*. This selection will affect the rest of the available selections. |
| **Data Bindings** | | The data bindings vary depending on the chart type selected. |
| **area or line graphs** | | |
| | **X-Axis** | *Data Binding*: Select a value from the drop-down list. The available options will vary depending on the selected dataset.<br>*Label*: Enter a label for the axis. |
| | **Add line** | Select to add more lines. |
| | **Lines** | Enter the following options for each line:<br>• *Data Binding*: Select a value from the drop-down list. The available options will vary depending on the selected dataset.<br>• *Format*: Select a format from the drop-down list: *Bandwidth*, *Counter*, *Default*, or *Severity*.<br>• *Type*: Select the type from the drop-down list: *Line Up* or *Line Down*.<br>• *Legend*: Enter the legend text for the line. |
| **bar** | | |
| | **X-Axis** | *Data Binding*: Select a value from the drop-down list. The available options will vary depending on the selected dataset.<br>*Only Show First*: Enter a numerical value. Only the first 'X' items will be displayed. Other items are bundled into the *Others* category.<br>*Overwrite label*: Enter a label for the axis. |
| | **Y-axis** | *Data Binding*: Select a value from the drop-down list. The available options will vary depending on the selected dataset.<br>*Overwrite label*: Enter a label for the axis. |
| | **Group By** | *Data Binding*: Select a value from the drop-down list. The available options will vary depending on the selected dataset.<br>*Show Top*: Enter a numerical value. Only the first 'X' items will be displayed. Other items can be bundled into the *Others* category. |
| | **Bundle rest into "Others"** | Select to bundle the rest of the results into an *Others* category. |
| | **Order By** | Select to order by the X-Axis or Y-Axis. |

| | | |
|---|---|---|
| **pie or donut graphs** | | |
| | **Category** | *Data Binding*: Select a value from the drop-down list. The available options will vary depending on the selected dataset.<br>*Label*: Enter a label for the axis.<br>*Show Top*: Enter a numerical value. Only the first 'X' items will be displayed. Other items can be bundled into the *Others* category. |
| | **Series** | *Data Binding*: Select a value from the drop-down list. The available options will vary depending on the selected dataset.<br>*Format*: Select a format from the drop-down list: *Bandwidth*, *Counter*, *Default*, *Percentage*, or *Severity*<br>*Label*: Enter a label for the axis. |
| | **Bundle rest into "Others"** | Select to bundle the rest of the results into an *Others* category. |
| **table** | | |
| | **Table Type** | Select *Regular*, *Ranked*, or *Drilldown*. |
| | **Add Column** | Select to add a column. Up to 15 columns can be added for a *Regular* table, *Ranked* tables have two columns, and *Drilldown* tables have three columns. |
| | **Columns** | The following column settings must be set:<br>• *Column Title*: Enter a title for the column.<br>• *Width*: Enter the column width as a percentage.<br>• *Add Data Binding*: Add data bindings to the column. Every column must have at least one data binding. The maximum number varies depending on the table type.<br>• *Data Binding*: Select a value from the drop-down list. The options vary depending on the selected dataset.<br>• *Format*: Select a value from the drop-down list. |
| | **Order By** | Select what to order the table by. The available options will vary depending on the selected dataset. |
| | **Bundle rest into "Others"** | Select to bundle the rest of the results into an *Others* category. This option is not available for regular tables. |
| | **Show Top** | Enter a numerical value. Only the first 'X' items will be displayed. Other items can be bundled into the *Others* category for *Ranked* and *Drilldown* tables. |
| | **Drilldown Top** | 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 |
|---|---|
| **Create New** | Create a new chart |
| **Edit** | Edit a chart. You can edit charts that you created. You cannot edit pre-defined charts. |
| **View** | Displays the settings for the selected predefined chart. You cannot edit a predefined chart. |
| **Delete** | Deletes the selected chart. You can delete charts that you create. You cannot delete predefined charts. |
| **Clone** | Clones the selected chart |
| **Import** | Import an exported FortiAnalyzer chart. |
| **Export** | Export one or more FortiAnalyzer charts. |
| **Show Predefined** | Displays the predefined charts |
| **Show Custom** | Displays the custom charts |
| **Search** | 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

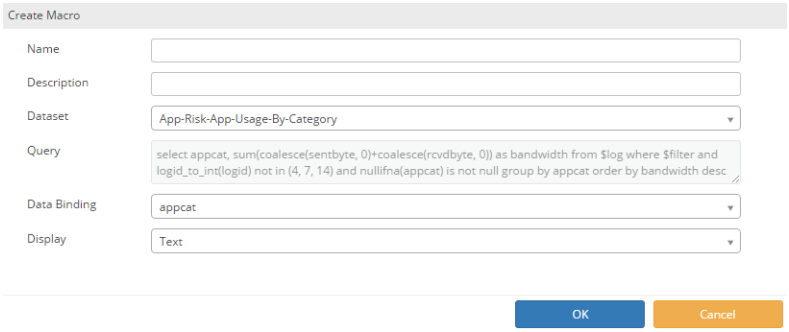
The FortiAnalyzer unit provides a selection of predefined macros. You can also create new macros, or clone and edit existing macros.

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.




3. Provide the required information for the new macro.

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

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 |
|---|---|
| **Create New** | Create a new macro |
| **Edit** | Edit the selected macro. You can edit macros that you created. You cannot edit predefined macros. |
| **View** | Displays the settings for the selected macro. You cannot edit a predefined macro. |
| **Delete** | Deletes the selected macro. You can delete macros that you create. You cannot delete predefined macros. |
| **Clone** | Clones the selected macro |
| **Show Predefined** | Displays the predefined macros |
| **Show Custom** | Displays the custom macros |
| **Search** | 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.

| | |
|---|---|
| **Name** | Enter a name for the dataset. |
| **Log Type** | Select a log type from the drop-down list.<br>• The following log types are available for FortiGate: *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*, and *GTP*.<br>• The following log types are available for FortiMail: *Email Filter*, *Event*, *History*, and *Virus*.<br>• The following log types are available for FortiWeb: *Intrusion Prevention*, *Event*, and *Traffic*. |
| **Query** | Enter the SQL query used for the dataset. |
| **Add Variable** | Click the *Add* button to add variable, expression, and description information. |
| **Test query with specified devices and time period** | |
| **Time Period** | Use the drop-down list to select a time period. When selecting *Other*, enter the start date, time, end date, and time. |
| **Devices** | Select *All Devices* or *Specify* to select specific devices to run the SQL query against. Click the *Select Device* button to add multiple devices to the query. |
| **Test** | 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.

### Validating datasets

We suggest you validate a dataset (especially a custom dataset) before using it in your report.

**To validate a dataset:**

1. Ensure you are in the correct ADOM, if using ADOMs. Otherwise, skip this step.
2. Go to *Reports* > *Report Definitions* > *Datasets*.
3. Select a dataset, and then click *Validate* in the toolbar.

Validation results are displayed in the Data Validation dialog box. If any error is detected, you can edit the dataset in the dialog box and then click *Save and Revalidate*.

You can also click *Validate All Custom* in the toolbar to validate all the custom datasets.

## Output profiles

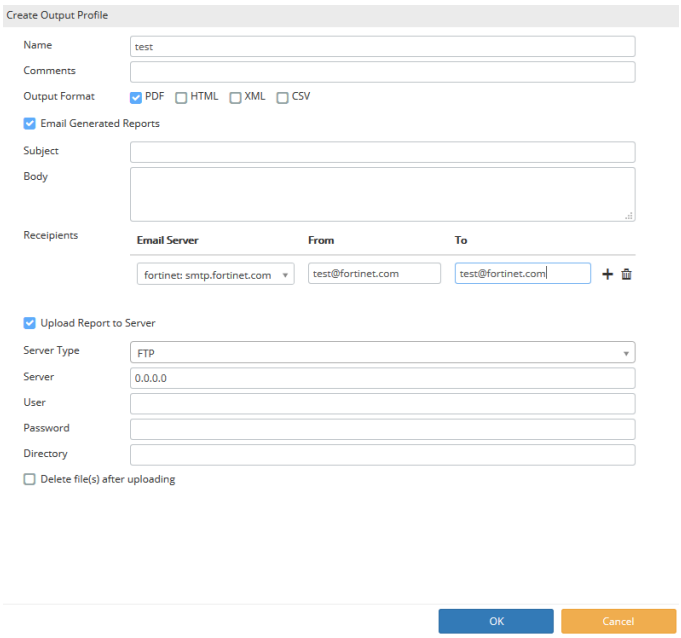
Output profiles allow you to define email addresses to which generated reports are sent and provide an option to upload the reports to FTP, SFTP, or SCP servers. Once created, an output profile can be specified for a report.

### Creating output profiles

You must configure a mail server before you can configure an output profile. See Mail servers on page 182.

**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.




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

| | |
|---|---|
| **Name** | Enter a name for the new output profile. |
| **Comments** | Enter a comment about the output profile (optional). |
| **Output Format** | Select the format or formats for the generated report. You can choose from PDF, HTML, XML, and CSV formats. |
| **Email Generated Reports** | Enable emailing of generated reports. |
| **Subject** | Enter a subject for the report email. |
| **Body** | Enter body text for the report email. |
| **Recipients** | Select the email server from the drop-down list and enter to and from email addresses.Select *Add New* to add another entry so that you can specify multiple recipients. |
| **Upload Report to Server** | Enable uploading of generated reports to a server. |
| **Server Type** | Select *FTP*, *SFTP*, or *SCP* from the drop-down list. |
| **Server** | Enter the server IP address. |
| **User** | Enter the username. |
| **Password** | Enter the password. |
| **Directory** | Specify the directory where the report will be saved. |
| **Delete file(s) after uploading** | Select to delete the 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 |
|---|---|
| **Create New** | Create a new output profile. |
| **Edit** | Edit the selected output profile. |
| **Delete** | 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 |
|---|---|
| **Create New** | Create a new report language placeholder. |
| **View** | View details about the selected report language. |
| **Edit** | Edit the selected report language. You cannot edit predefined report languages. |
| **Delete** | Delete the selected report language. You cannot delete predefined report languages. |

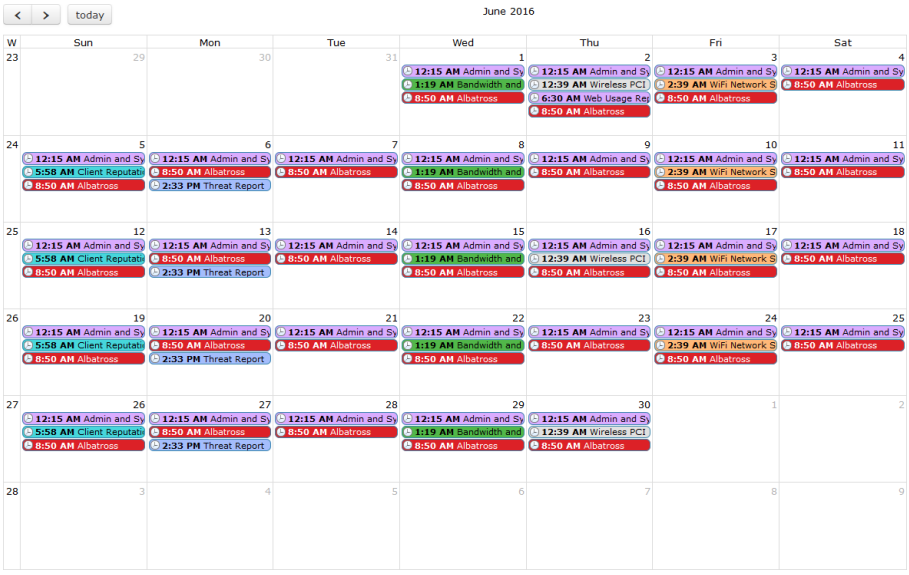
# Report calendar

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 |
| Template - FortiClient Vulnerability Scan Report | |

### FortiCache report templates

| |
|---|
| Template - FortiCache Default Report |

### FortiCarrier report templates

| |
|---|
| Template - FortiCarrier Default Report |

### FortiClient EMS report templates

| |
|---|
| Template - FortiClient Default Report |
| Template - FortiClient Vulnerability Scan 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 |
| Template - FortiWeb Web Application Analysis Report |

## Reports Settings tab

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

| Field | Description |
|---|---|
| **Time Period** | The time period that the report will cover. Select a time period, or select *Other* to manually specify the start and end date and time. |
| **Devices** | The devices that the report will include. Select either *All Devices* or *Specify* to add specific devices. Select the add icon to select devices. |
| **Type** | Select either *Single Report (Group Report)* or *Multiple Reports (Per-Device)*.<br>This option is only available if multiple devices are selected. |
| **Enable Schedule** | Select to enable report template schedules. |
| **Enable Auto-Cache** | 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. |
| **Generate PDF Report Every** | Select when the report is generated.<br>Enter a number for the frequency of the report based on the time period selected from the drop-down list. |
| **Start time** | Enter a starting date and time for the file generation. |
| **End time** | Enter an ending date and time for the file generation, or set it for never ending. |
| **Enable Notification** | Select to enable report notification. |
| **Output Profile** | Select the output profile from the drop-down list, or select *Create New* to create a new output profile. See Output profiles on page 138. |

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

### Advanced Settings section of Reports Settings tab

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

| Field | Description |
|---|---|
| **Language** | Select the report language. Select one of the following: *Default, English*, *French*, *Japanese*, *Korean*, *Portuguese*, *Simplified_Chinese*, *Spanish*, or *Traditional_Chinese*. |
| **Bundle rest into "Others"** | Select to bundle the uncategorized results into an *Others* category. |
| **Print Orientation** | Set the print orientation to portrait or landscape. |
| **Chart Heading Level** | Set the heading level for the chart heading. |
| **Hide # Column** | Select to hide the column numbers. |
| **Layout Header** | Enter header text and select the header image. The default image is *fortinet_logo.png*. |
| **Layout Footer** | Select either a default footer or custom footer. When selecting *Custom*, enter the footer text in the text field. |
| **Print Cover Page** | Select to print the report cover page. Select *Customize* to customize the cover page. See Customizing report cover pages on page 126. |
| **Print Table of Contents** | Select to include a table of contents. |
| **Print Device List** | Select to print the device list. Select *Compact*, *Count*, or *Detailed* from the drop-down list. |

| Field | Description |
|---|---|
| **Print Report Filters** | Select to print the filters applied to the report. |
| **Obfuscate User** | Select to hide user information in the report. |
| **Resolve Hostname** | Select to resolve hostnames in the report. The default status is *disabled*. |
| **Allow Save Maximum** | Select a value between 1-10000 for the maximum number of reports to save. |
| **Color Code** | The color used to identify the report on the calendar. Select a color code from the drop-down list to apply to the report schedule. Color options include: *Bold Blue*, *Blue*, *Turquoise*, *Green*, *Bold Green*, *Yellow*, *Orange*, *Red*, *Bold Red*, *Purple*, and *Gray*. |

## 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 |
|---|---|
| **Save as Template** | Select the save the layout as a template. |
| **Cut** | To cut a text fragment, start with selecting it. When the text is selected, you can cut it using one of the following methods:<br>• Select the cut button in the toolbar<br>• Right-click and select cut in the menu<br>• Use the *CTRL+X* shortcut on your keyboard. |
| **Copy** | To cut a text fragment, start with selecting it. When the text is selected, you can cut it using one of the following methods:<br>• Select the cut button in the toolbar<br>• Right-click and select cut in the menu<br>• Use the *CTRL+C* shortcut on your keyboard. |
| **Paste** | To paste a text fragment, start with cutting it or copying from another source. Depending on the security settings of your browser, you may either paste directly from the clipboard or use *Paste* dialog window. |

| Field | Description |
|---|---|
| **Paste as plain text** | If you want to paste an already formatted text, but without preserving the formatting, you can paste it as plain text. To achieve this, copy the formatted text and select the *Paste as plain text* button in the toolbar. If the browser blocks the editor toolbar's access to clipboard, a *Paste as Plain Text* dialog window will appear and you will be asked to paste the fragment into the text box using the *CTRL+V* keyboard shortcut. |
| **Paste from Word** | You can preserve basic formatting when you paste a text fragment from Microsoft Word. To achieve this, copy the text in a Word document and paste it using one of the following methods:<br>• Select the Paste from Word button in the toolbar<br>• Use the *CTRL+V* shortcut on your keyboard. |
| **Undo** | Select to undo the last action. Alternatively, use the *CTRL+Z* keyboard shortcut to perform the undo operation. |
| **Redo** | Select to redo the last action. Alternatively, use the *CTRL+Y* keyboard shortcut to perform the redo operation. |
| **Find** | Select to find text in the report layout editor. Find consists of the following elements:<br>• Find what: Is the text field where you enter the word or phrase that you want to find.<br>• 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.<br>• Match whole word: Checking this option limits the search operation to whole words.<br>• 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. |

| Field | Description |
|---|---|
| **Replace** | Select to replace text in the report layout editor. Replace consists of the following elements:<br>• Find what: Is the text field where you enter the word or phrase that you want to find.<br>• Replace with: Is the text field where you enter the word or phrase that will replace the search term in the document.<br>• 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.<br>• Match whole word: Checking this option limits the search operation to whole words.<br>• Match cyclic: Checking this option means that after editor reaches the end of the document, the search continues from the beginning of the text. This option is checked by default. |
| **Image** | Select the *Image* button in the toolbar to insert an image into the report layout. Right-click an existing image to edit image properties. |
| **Table** | Select the *Table* button in the toolbar to insert a table into the report layout. Right-click an existing table to edit a cell, row, column, table properties or delete the table. |
| **Insert Horizontal Line** | Select to insert a horizontal line. |
| **Insert Page Break for Printing** | Select to insert a page break for printing. |
| **Link** | Select the *Link* button in the toolbar to open the *Link* dialog window. You can select to insert a URL, a link to an anchor in the text, or an email address. Alternatively, use the *CTRL+L* keyboard shortcut to open the *Link* dialog window. |
| **Anchor** | Select the *Anchor* button in the toolbar to insert an anchor in the report layout. |
| **FortiAnalyzer Chart** | Select to insert a FortiAnalyzer chart. Charts are associated with datasets that extract data from logs for the report. |
| **FortiAnalyzer Macro** | Select to insert a FortiAnalyzer macro. Macros are associated with datasets that extract data from logs for the report. |
| **Paragraph Format** | Select the paragraph format from the drop-down list. Select one of the following: Normal, Heading 1, Heading 2, Heading 3, Heading 4, Heading 5, Heading 6, Formatted, or Address. |

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

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

# 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

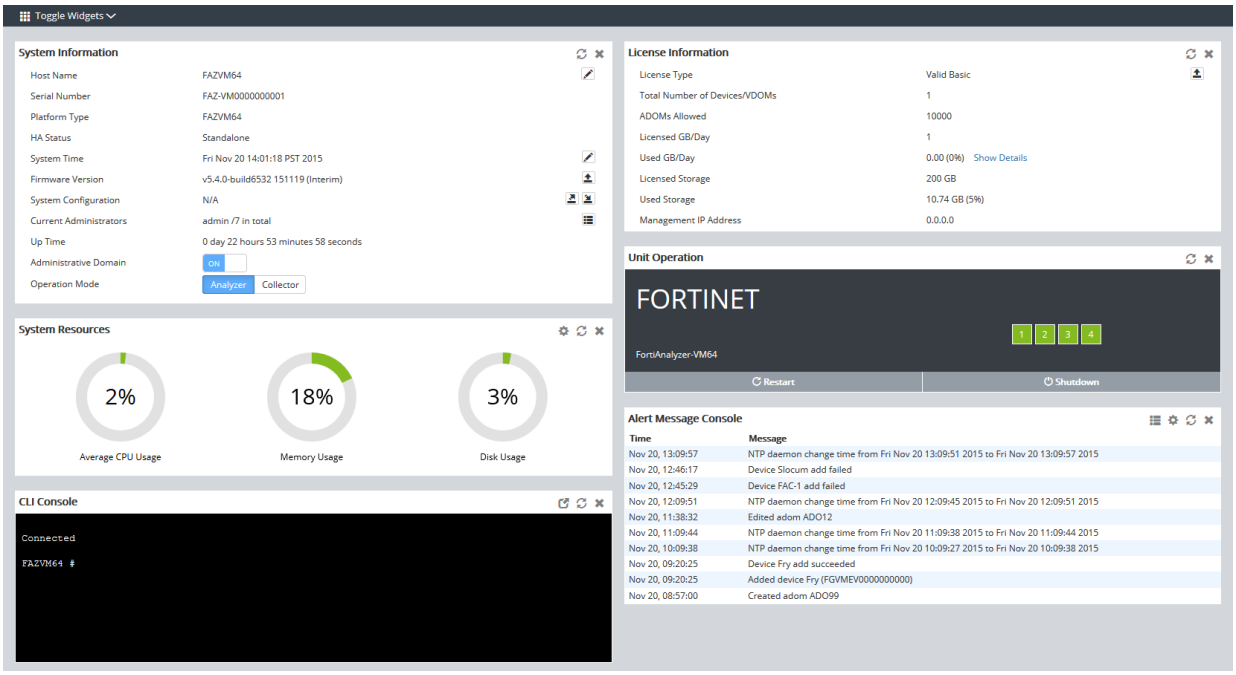
You can access the following options by using the tree menu on the *System Settings* pane:

| Option | Description |
|---|---|
| **Dashboard** | Displays the system settings dashboard. See System settings dashboard on page 152. |
| **All ADOMs** | Available when administrative domains (ADOMs) are enabled. You can create, edit, and monitor all ADOMs. See Administrative Domains on page 43. |
| **Storage Info** | Displays information about how much FortiAnalyzer disk space has been used for log storage. You can configure and monitor log storage settings. See . |
| **Network** | Displays the FortiAnalyzer network settings. See Network on page 31. |
| **Admin** | Expand and collapse to display and hide access to the following administrator settings for FortiAnalyzer: |
| **Administrators** | Displays the administrator accounts. See Administrator Accounts on page 51. |
| **Profile** | Displays the administrator profiles. See Administrator profiles on page 55. |
| **Remote Auth Server** | Displays the configured remote authorization servers. See Remote authentication servers on page 56. |
| **Admin Settings** | Displays the global administrator settings. See Admin settings on page 63. |
| **Certificates** | Expand and collapse to display and hide access to the following certificate settings: |
| **Local Certificates** | View and manage local certificates. See Local Certificates on page 160. |

| Option | Description |
|---|---|
| **CA Certificates** | View and manage CA certificates. See CA Certificates on page 162. |
| **CRL** | View and manage Certificate Revocation Lists (CRLs). See Certificate revocation lists on page 163. |
| **Log Forwarding** | Displays the log forwarding configurations. See Log Forwarding on page 164. |
| **Fetcher Management** | Displays configurations for fetching or receiving logs from another FortiAnalyzer unit. See Log fetcher management on page 167. |
| **Event Log** | Displays the event log for FortiAnalyzer. See FortiAnalyzer event log on page 170. |
| **Task Monitor** | Displays the task monitor for FortiAnalyzer. See FortiAnalyzer task monitor on page 173. |
| **Advanced** | Expand and collapse to display and hide access to the following advanced settings: |
| **SNMP** | Displays configured SNMP servers. See SNMP on page 175. |
| **Mail Server** | Displays configured mail servers. See Mail servers on page 182. |
| **Syslog Server** | Displays configured syslog servers. See Syslog servers on page 183. |
| **Meta Fields** | Displays options for meta fields. See Meta fields on page 183. |
| **Device Log Settings** | Displays device log settings. See Configuring rolling and uploading of logs on page 84. |
| **File Management** | Displays global automatic deletion settings. See Configuring global automatic deletion on page 83. |
| **Advanced Settings** | Displays advanced settings, such as changing the ADOM mode, downloading the WSDL file, and specifying the size of the task list. See WSDL files on page 184. |

## 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 |
|---|---|
| **System Information** | 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.<br>From this widget you can manually update the FortiAnalyzer firmware to a different release. For more information, see .<br>The widget fields will vary based on how the FortiAnalyzer is configured, for example, if ADOMs are enabled. |
| **System Resources** | Displays the real-time and historical usage status of the CPU, memory, and hard disk. For more information, see Viewing CPU status on page 157. |
| **License Information** | Displays the devices being managed by the FortiAnalyzer unit and the maximum numbers of devices allowed. For more information, see .<br>From this widget you can manually upload a license for FortiAnalyzer VM systems. |
| **Unit Operation** | 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 Viewing port status on page 157. |
| **CLI Console** | Opens a terminal window that enables you to configure the FortiAnalyzer unit using CLI commands directly from the GUI. For more information, see Accessing the CLI on page 160. |

| Widget | Description |
|---|---|
| **Alert Message Console** | Displays log-based alert messages for both the FortiAnalyzer unit itself and connected devices. For more information, see Viewing and updating FortiAnalyzer firmware on page 155. |
| **Log Receive Monitor** | Displays a real-time monitor of logs received. You can select to view data per device or per log type. See Viewing the number of logs being received on page 158. |
| **Insert Rate vs Receive Rate** | Displays the log insert log receive rates in a line graph.<br>• Log receive rate: how many logs are being received.<br>• Log insert rate: how many logs are being actively inserted into the database.<br>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.<br>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). |
| **Log Insert Lag Time** | 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. |
| **Disk I/O** | Displays the disk utilization, transaction rate, or throughput as a percentage over time.<br>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. |

## 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 |
|---|---|
| **Move a widget** | Move the widget by clicking and dragging its title bar, then dropping it in its new location |
| **Add a widget** | Select *Toggle Widgets* from the toolbar, then select the name widget you need to add. |
| **Delete a widget** | Click the *Close* icon in the widget's title bar. |
| **Customize a widget** | For widgets with an (Edit) icon, you can customize the view by clicking the Edit icon and configuring the settings. |

| Action | Steps |
|---|---|
| **Reset the dashboard** | Select *Toggle Widgets* > *Reset to Default* 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 Two operation modes on page 18.

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

**To change the operation mode:**

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

## Viewing and updating FortiAnalyzer firmware

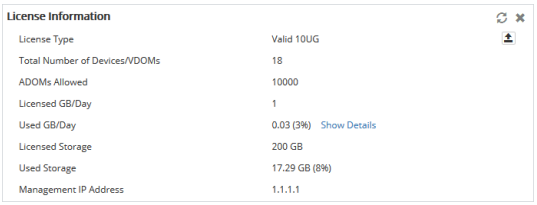
The version and build numbers of the firmware installed on the FortiAnalyzer unit are listed in the *Firmware Version* field in the *System Information* widget. To take advantage of the latest features and fixes, the device firmware can be updated.

You can download the latest version from the Customer Service & Support portal at https://support.fortinet.com. After your download the latest version to your management computer, click the *Upgrade Firmware* icon of the *Firmware Version* field, and select the firmware image to load. For more information, see the *FortiAnalyzer Upgrade Guide* .

## 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.



## 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.

## Enabling FortiAnalyzer to manage a small number of FortiGate devices

You can enable FortiManager features on FortiAnalyzer so that it can manage a small number of FortiGate devices. All the FortiManager features can be enabled on FortiAnalyzer except FortiGuard.

The free license that comes with your FortiAnalyzer unit enables it to manage two FortiGate devices when FortiManager features are enabled. You can purchase a management license to enable your FortiAnalyzer unit to manage up to 20 FortiGate devices.

The upgrade license is supported only on FortiAnalyzer 2U and above devices.

You can enable FortiManager features by using either GUI or CLI.

**To enable FortiManager features on FortiAnalyzer using GUI:**

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, toggle the *FortiManager Features* switch to *On*.
3. After the system reboots, log in to the FortiAnalyzer GUI.

The FortiAnalyzer home page now also shows FortiManager feature tiles except FortiGuard.

**To enable FortiManager features on FortiAnalyzer using CLI:**

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

```
config system global
set fmg-status enable
end
```

The following prompt is displayed:

```
Changing fmg status will affect FAZ feature. If you continue, system
will reboot.
Do you want to continue? (y/n)
```

Type `Yes`.

2. After the system reboots, log in to the FortiAnalyzer GUI. FortiManager features except FortiGuard have been enabled.

After FortiManager features are enabled, you can upgrade the management license so that your FortiAnalyzer unit can manage up to 20 FortiGate devices.

**To upgrade the management license:**

1. Go to *System Settings* > *Dashboard*.
2. In the *License Information* widget, find the *Management* > *Devices/VDOMs* field and click the *Upload license* icon.
3. In the dialog box that opens, provide the license key that you have purchased.

You can disable the FortiManager features on your FortiAnalyzer at any time, by using GUI or CLI.

**To disable FortiManager features on FortiAnalyzer using GUI:**

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, toggle the *FortiManager Features* switch to *Off*.
3. After the system reboots, log in to the FortiAnalyzer GUI.

The FortiAnalyzer home page changes back and no longer shows FortiManager feature tiles.

**To disable FortiManager features on FortiAnalyzer using CLI:**

- From the CLI, or in the CLI Console widget, enter the following :

```
config system global
set fmg-status disable
end
```

The following prompt is displayed:

```
Changing fmg status will affect FAZ feature. If you continue, system
will reboot.
Do you want to continue? (y/n)
```

Type `Yes`.

## 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.

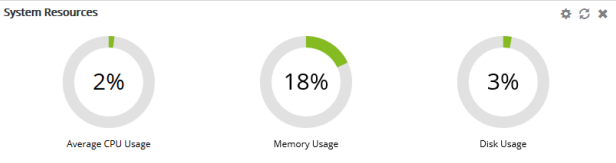
Hover the cursor over the ports to view a pop-up that displays the full name of the interface, the IP address and netmask, the link status , the speed of the interface, and the amounts of sent and received data.

## 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*.

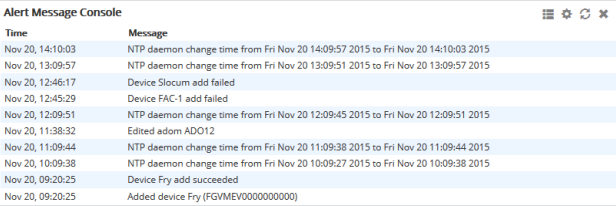
To view individual CPU usage, from the Real-Time display, click on the CPU chart. To go back to the standard view again, click the chart again.




## 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.



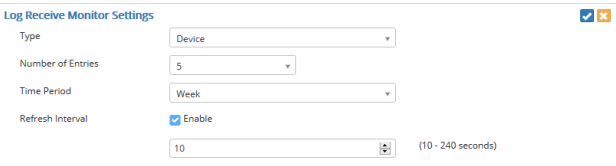

Click *Edit* from the widget toolbar to view the *Alert Message Console Settings*, where you can adjust the number of entries that are visible in the widget, and the refresh interval.

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 a specified time period, as well as the average rate. You can select to display log data by log type or device.

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




## 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:

| | |
|---|---|
| **System Time** | The date and time according to the FortiAnalyzer unit's clock at the time that this tab was loaded or when you last clicked the *Refresh* button. |
| **Time Zone** | Select the time zone in which the FortiAnalyzer unit is located and whether or not the system automatically adjusts for daylight savings time. |
| **Update Time By** | Select *Set time* to manually set the time, or *Synchronize with NTP Server* to automatically synchronize the time. |
| **Set Time** | Manually set the data and time. |
| **Select Date** | Set the date from the calendar or by manually entering it in the format: YYY/MM/DD. |
| **Select Time** | Select the time. |
| **Synchronize with NTP Server** | Automatically synchronize the date and time. |
| **Sync Interval** | 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. |
| **Server** | 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 http://www.ntp.org. |

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.

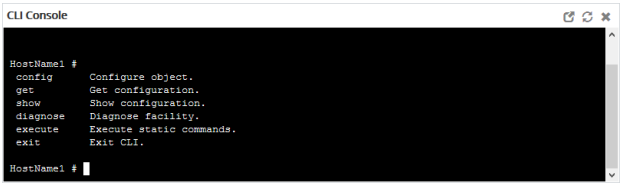
## Accessing the CLI

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.




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

# 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:

| | | |
|---|---|---|
| **Certificate Name** | | The name of the certificate. |
| **Subject Information** | | Select and then enter the ID Type (*Host IP*, *Domain Name*, or *Email*). |
| **Optional Information** | | |
| | **Organization Unit (OU)** | 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. |
| | **Organization (O)** | Legal name of the company or organization. |
| | **Locality (L)** | Name of the city or town where the device is installed. |
| | **State/Province (ST)** | Name of the state or province where the FortiGate unit is installed. |
| | **Country (C)** | Select the country where the unit is installed from the drop-down list. |
| | **E-mail Address (EA)** | Contact email address. |
| | **Subject Alternative Name** | Optionally, enter one or more alternative names for which the certificate is also valid. Separate names with a comma.<br>A name can be:<br>• e-mail address<br>• IP address<br>• URI<br>• DNS name (alternatives to the Common Name)<br>• directory name (alternatives to the Distinguished Name)<br>You must precede the name with the name type. |
| **Key Type** | | The key type can be *RSA* or *Elliptic Curve*. |
| **Key Size** | | Select the key size from the drop-down list: *512 Bit*, *1024 Bit*, *1536 Bit*, or *2048 Bit*. Only available when the key type is *RSA*. |
| **Curve Name** | | Select the curve name from the drop-down list: secp256r1, secp384r1, or secp521r1. Only available when the key type is *Elliptic Curve*. |
| **Enrollment Method** | | The enrollment method is set to *File Based*. |

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

## Importing local certificates

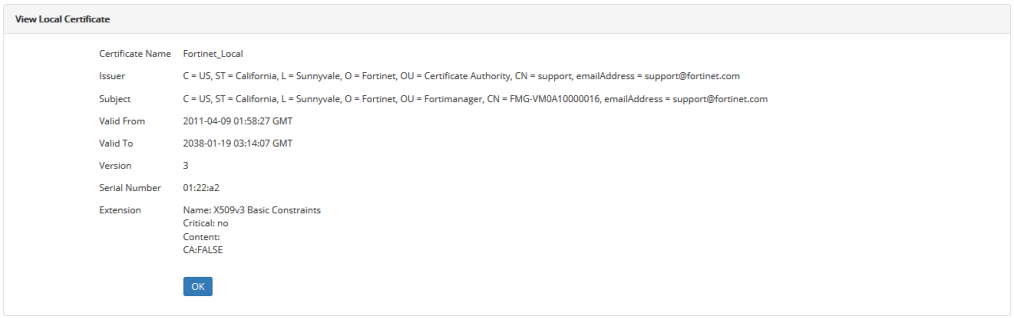
**To import a local certificate:**

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 forward logs from a FortiAnalyzer unit 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 plays the role of the *client*, and the FortiAnalyzer unit, syslog server, or CEF server that receives logs plays the role of the *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 Archive logs on the FortiAnalyzer unit. See also Log storage on page 20.

### Modes

FortiAnalyzer supports the following log forwarding modes.

**Real-time**

Logs are forwarded as they are received. FortiAnalyzer supports real-time log forwarding to another FortiAnalyzer unit, a syslog server, or a CEF server. *Content files*, which include DLP (data leak prevention) files, antivirus quarantine files, and IPS (intrusion prevention system) packet captures, are NOT forwarded.

Real-time mode is the default mode.

**Aggregation**

As FortiAnalyzer receives logs from devices, it stores them, and then forwards the logs at a specified time everyday. In this mode, *content files* are also forwarded daily at the scheduled time.

FortiAnalyzer supports log forwarding in aggregation mode only between two FortiAnalyzer units. Syslog and CEF servers are not supported.

**Mixed (Both)**

Logs are forwarded in real-time, while content files are forwarded in aggregation at a specified time daily.

For both Aggregation and Mixed modes, the client needs to provide the login credentials of an administrator account of the server with a Super_User profile to get authenticated by the server to forward logs.

### Configuring log forwarding mode in CLI

You can use the following CLI command to configure the log forwarding mode:

```
config system aggregation-client
edit [log aggregation ID]
set mode [realtime, aggregation, both, or disable]
end
```

## Configuring log forwarding

### Configuring the server

**To configure the server (the FortiAnalyzer unit or Syslog/CEF server that *receives* logs):**

1. (For Aggregation and Mixed modes) Prepare an administrator account with a *Super_User* profile. (You can use the default admin account, which is assigned the *Super_User* profile, or create a custom administrator account.) The client will need to provide the login credentials of this Administrator account to get authenticated by the server. See also Configuring administrator accounts on page 53.
2. Add the devices for which the client will forward logs. See also Adding devices on page 69.
3. (For Aggregation and Mixed modes) Enable the log aggregation service on the server side.
   a. Go to *System Settings* > *Dashboard*.
   b. In the *CLI Console* widget, enter the following CLI commands:

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

## Configuring the client

Log forwarding is enabled by default. If you cannot see *System Settings* > *Log Forwarding* in the GUI, you will have to enable it first.

When a FortiAnalyzer unit works in the Collector mode, log forwarding is always enabled. You cannot disable it.

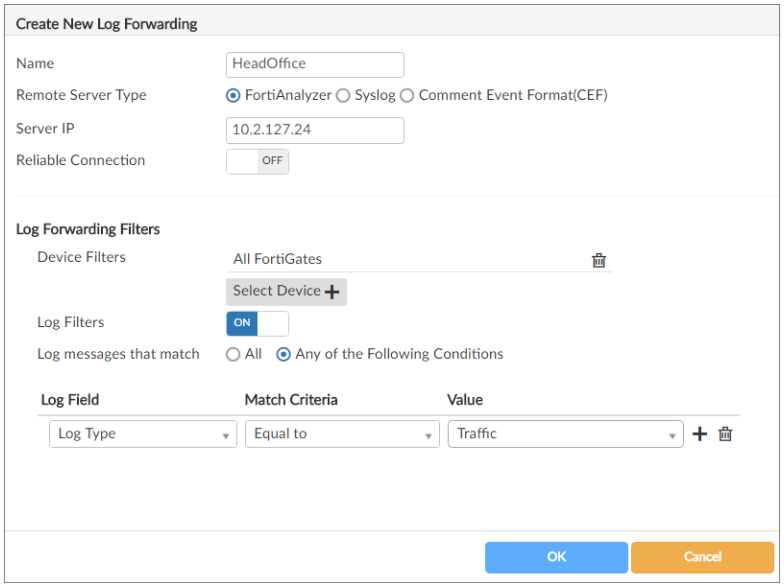
**To enable log forwarding:**

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
```

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

1. Go to *System Settings* > *Log Forwarding*, and click *Create New*.
2. In the *Create New Log Forwarding* pane that is displayed, configure the settings:




| | |
|---|---|
| **Name** | Provide a name for the remote server. |
| **Remote Server Type** | Select the type of remote server to which you are forwarding logs. *FortiAnalyzer*, *Syslog*, or *Common Event Format (CEF)*. |
| **Server IP** | Enter the IP address of the remote server. |
| **Server Port** | Enter the server port. When *Remote Server Type* is *FortiAnalyzer*, you cannot change the port. The default port 514 is used. |

| | |
|---|---|
| **Reliable Connection** | Toggle the switch on to enable TCP connection. UDP connection is used if the switch is off. |
| **Log Forwarding Filters** | |
| **Device Filters** | Click *Select Device* and then add devices for which to forward logs. |
| **Log Filters** | Toggle the switch on to filter the logs that are forwarded in real-time. Add a filter by completing the *Log Field*, *Match Criteria*, and *Value* options. |
| **Enable Exclusions** | This option is available when the remove server is a Syslog or CEF server. Toggle the switch on and then add an exclusion by completing the *Device Type*, *Log Type*, and *Exclusion List* options. To add an *Exclusion List*, click *Fields*, and specify the log fields that you want to exclude in the *Select Log Field* pane that opens. |

The client will forward logs in realtime mode by default. You can change the mode in CLI. See Configuring log forwarding mode in CLI on page 165.

3. Click *OK*.

The client starts to forward logs to the server. If real-time forwarding has been configured, you can check the forwarded logs on the server side immediately.

# Log fetcher management

## About log fetching

You can enable one FortiAnalyzer to fetch Archive logs of specified devices from another FortiAnalyzer. The FortiAnalyzer device that fetches logs operates as the *fetch client*, and the other FortiAnalyzer device that sends logs operates as the *fetch server*.

Log fetching can only happen between two FortiAnalyzer devices, and both of them must be running the same FortiAnalyzer version, i.e., 5.4.1. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with different FortiAnalyzer devices at the other end. Only one log fetching session can be established at a time between two FortiAnalyzer devices.

## Conducting log fetching between two FortiAnalyzer units

Conducting log fetching between two FortiAnalyzer devices involves the following steps:

1. On the fetch client, create a profile for the fetch server. See Creating a profile for the fetch server on page 168.
2. On the fetch client, send the fetch request. See Sending a fetch request to the fetch server on page 168
3. (First-time fetch from the device, or any changes have been made to the devices and/or ADOMs since the last fetch) On the fetch client, use the *Sync Device* feature to sync devices and ADOMs with the server. See Syncing devices with the fetch server on page 169.
4. On the fetch server, review the fetch request, and then approve or reject it. See Processing the fetch request on

the fetch server on page 170

5. Monitor the fetch progress. See Monitoring the fetch progress on page 170.

## Creating a profile for the fetch server

**To create a fetch profile:**

1. On the fetch client, go to *System Settings* > *Fetcher Management*.
2. In the *Profiles* tab, click *Create New*.
3. In the *Create New* dialog box that opens, configure the settings.

| | |
|---|---|
| **Name** | Type a name for the profile. |
| **Server IP** | Type the IP address of the fetch server. |
| **User** | Provide the username of a fetch server administrator, which, together with the password, authenticates the fetch client's access to the fetch server. |
| **Password** | Provide the login password of a fetch server administrator, which, together with the username, authenticates the fetch client's access to the fetch server. |
| **Note:** The fetch server administrator must have a *Standard_User* or *Super_User profile* to authenticate fetch requests. | |

4. Click *OK*.

## Sending a fetch request to the fetch server

**To send a fetch request:**

1. In the *Profiles* tab, select the profile of the fetch server, and click *Request Fetch*.
2. In the Fetch Logs dialog box, configure the settings.

| | |
|---|---|
| **Name** | Displays the name of the fetch server that you have specified. |
| **Server IP** | Displays the IP address of the fetch server that you have specified. |
| **User** | Displays the username of the fetch server administrator that you have provided. |
| **Secure Connection** | Enable this to use SSL connection to transfer fetched logs from the server. |
| **Server ADOM** | Select a server ADOM from the drop-down list, from which the client will fetch logs. You can select one server ADOM at a time. |
| **Local ADOM** | Specify the client ADOM to which the logs will be sent. Select an existing ADOM from the drop-down list, or create a new ADOM by typing the new ADOM name in the field. |

| | |
|---|---|
| **Devices** | Add the devices of which the client will fetch logs. Click *Select Device*, (search and) select the devices, and click *OK*. |
| **Enable Filters** | You can filter the logs to fetch by enabling and adding log filters. |
| **Time Period** | Specify what time range of log messages to fetch. |
| **Index Fetch Logs** | If selected, the fetched logs will be indexed in the SQL database of the fetch client once they are received. Select this option unless you want to manually index the fetched logs. |

**Maximum devices**
You can add up to 256 devices when creating a fetch profile. If you add more than 256 devices, the system will give an error message and the fetch profile cannot be created.

**Data policy**
If you are fetching logs to an existing local ADOM, make sure the ADOM has enough disk space for the upcoming logs. You also need to ensure that the data policy for the local ADOM supports fetching logs of the specified time period. That is, it keeps both Archive and Analytics logs long enough so that the fetched logs will not be deleted according to the policy.
For example, today is June 1, and the data policy of the local ADOM keeps Analytics 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 Analytics and Archive 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.

3. Click *Request Fetch*.

The fetch request is sent to the fetch server. You can view the request in the *Sessions* tab.

## Syncing devices with the fetch server

If this is the first time the client fetches logs from the device, or you have made any changes to the devices and/or ADOMs since the last fetch, you have to sync devices and ADOMs with the server. In 5.4.1, the *Sync Device* function takes care of this.

**To sync devices:**

- In the *Profiles* tab, select the fetch server profile, and click *Sync Devices*.

Once the sync is completed, you can verify the device and/or ADOM changes on the client. For example, you can find the newly added devices in the specified ADOM.

If a new ADOM is created, the new ADOM will mirror the disk space and data policy of the corresponding server ADOM. If there is not enough space on the client, the client will create an ADOM with the maximum allowed disk space and give a warning message. You can then adjust disk space allocation if you want.

### Processing the fetch request on the fetch server

**To process the fetch request:**

1. Go to the *Notification Center* and click the log fetcher request notification to open the request. Alternatively, you can go to *System Settings* > *Fetcher Management*, and find the request in the *Sessions* tab.
2. Click *Review* to review the request, and then click *Approve* or *Reject*.

If you approve the request, the fetch server will start to retrieve the requested Archive logs in the background and send the logs to the fetch client.

### Monitoring the fetch progress

You can monitor the fetch status on either the fetch server or fetch client, under the *Received Sessions* tab or the *Sent Sessions* tab respectively. You can pause the session by clicking *Pause*, and then resume the session by clicking *Resume*.

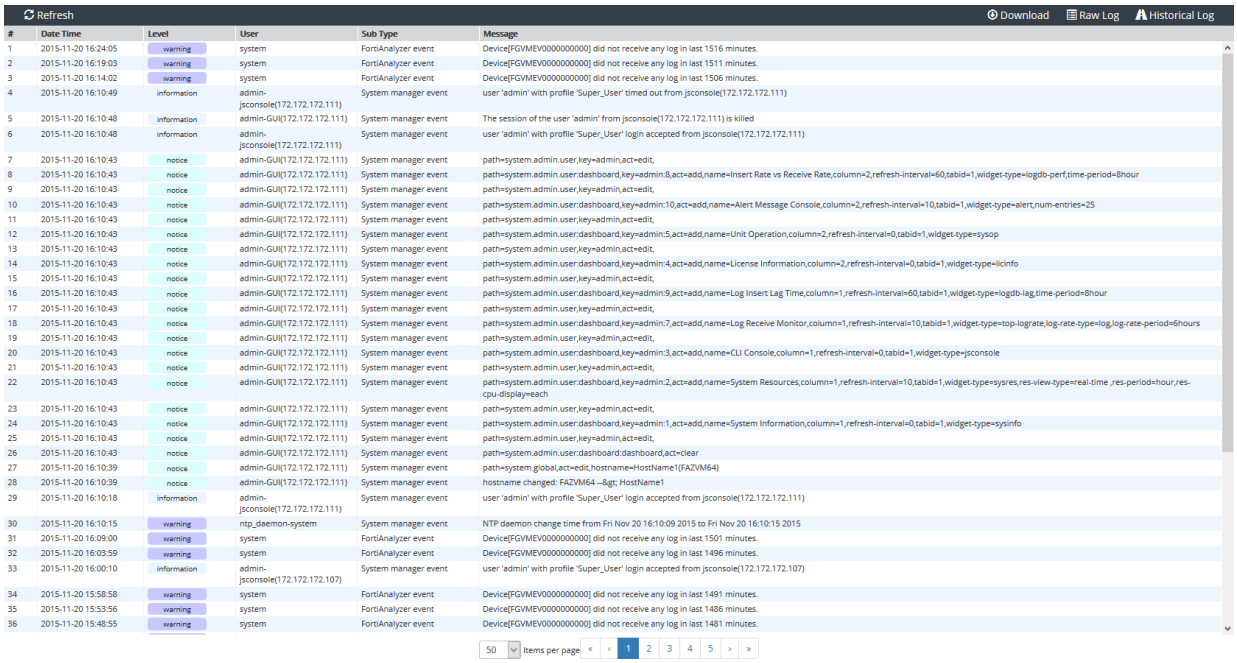
Once the log fetching is completed, the status is changed to Done. You can find the fetched logs in the *Log Browse* of *Log View*. The fetch client will then start to index the logs into the SQL database.

It takes some time for the fetch client to finish indexing the fetched logs and make the analyzed data available in features such as *FortiView* , *Event Monitor*, and *Reports*. You use CLI command `diagnose sql status rebuild-db` to check the SQL database rebuild status.

## 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.




The following information is displayed:

| | |
|---|---|
| **#** | The log number. |
| **Date Time** | The date and time that the log file was generated. |
| **Level** | The log level:<br>• Debug<br>• Information<br>• Notification<br>• Warning<br>• Error<br>• Critical<br>• Alert<br>• Emergency |
| **User** | User information. |

| | |
|---|---|
| **Sub Type** | The log sub-type:<br>System manager event, HA event<br>FG-FM protocol event, Firmware manager event<br>Device configuration event, FortiGuard service event<br>Global database event, FortiClient manager event<br>Script manager event, FortiMail manager event<br>Web portal event, Debug I/O log event<br>Firewall objects event, Configuration change event<br>Policy console event, Device manager event<br>VPN console event, Web service event<br>Endpoint manager event, FortiAnalyzer event<br>Revision history event, Log daemon event<br>Deployment manager event, FIPS-CC event<br>Real-time monitor event, Managered devices event<br>Log and report manager event |
| **Message** | Log message details. |

The following options are available:

| | |
|---|---|
| **Add Filter** | Filter the event log list based on the log level, user, sub type, or message. |
| **Download** | Download the event logs in either CSV or the normal format. |
| **Raw Log / Formatted Log** | Click on *Raw Log* to view the logs in their raw state. Click *Formatted Log* to view them in the formatted into a table. |
| **Historical Log** | Click to view the historical logs list. |
| **View** | View the selected log file. This option is only available when viewing historical event logs. |
| **Delete** | Delete the selected log file. This option is only available when viewing historical event logs. |

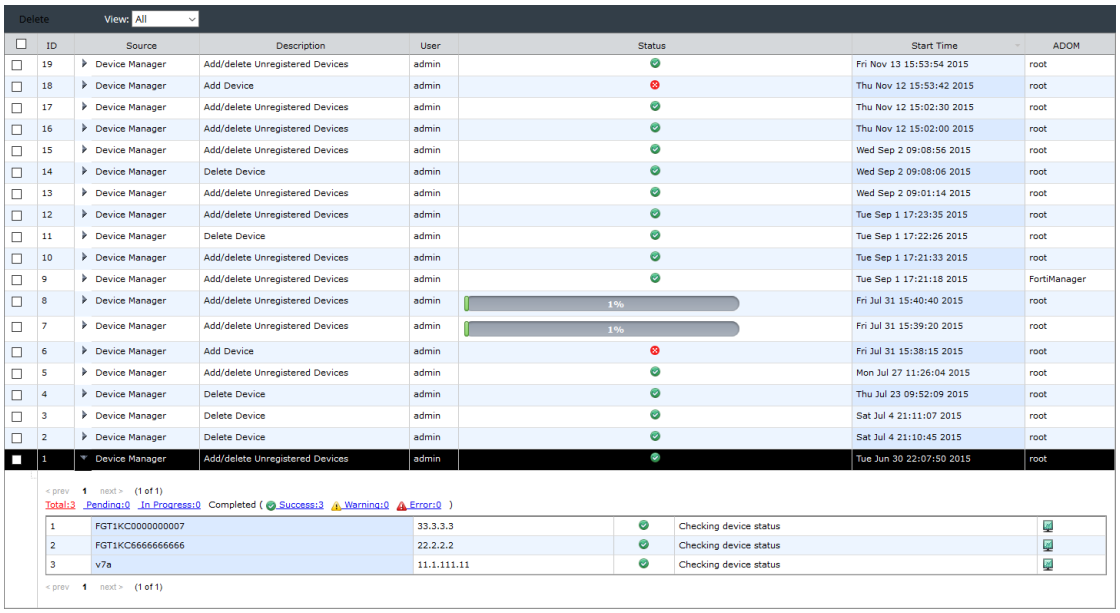
| | |
|---|---|
| **Clear** | Clear the selected file of logs. This option is only available when viewing historical event logs. |
| **Type** | Select the type from the drop down list. This option is only available when viewing historical logs.<br>Select one of the following: *Event Log*, *FDS Upload Log*, or *FDS Download Log*.<br>• *FDS Upload Log*: Select the device from the drop-down list.<br>• *FDS Download Log*: Select the service (*FDS*, or *FCT*) from the *Service* drop-down list, select the event type (*All Event*, *Push Update*, *Poll Update*, or *Manual Update*) from the *Event* drop-down list, and then click *Go* to browse logs. |
| **Search** | Enter a search term to search the historical logs. This option is only available when viewing historical event logs. |
| **Pagination** | 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.



The following information is available:

| | |
|---|---|
| **ID** | The identification number for a task. |
| **Source** | The platform from where the task is performed. Click the expand arrow to view details of the specific task and access the history button. |
| **Description** | The nature of the task. Click the arrow to display the specific actions taken under this task. |
| **User** | The user or users who performed the tasks. |
| **Status** | The status of the task (hover over the icon to view the description):<br>• *Done*: Completed with success.<br>• *Error*: Completed without success.<br>• *Canceled*: User canceled the task.<br>• *Canceling*: User is canceling the task.<br>• *Aborted*: The FortiAnalyzer system stopped performing this task.<br>• *Aborting*: The FortiAnalyzer system is stopping performing this task.<br>• *Running*: Being processed. In this status, a percentage bar appears in the Status column.<br>• *Pending*<br>• *Warning* |
| **Start Time** | The time that the task was started. |
| **ADOM** | The ADOM associated with the task. |
| **History** | 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*.

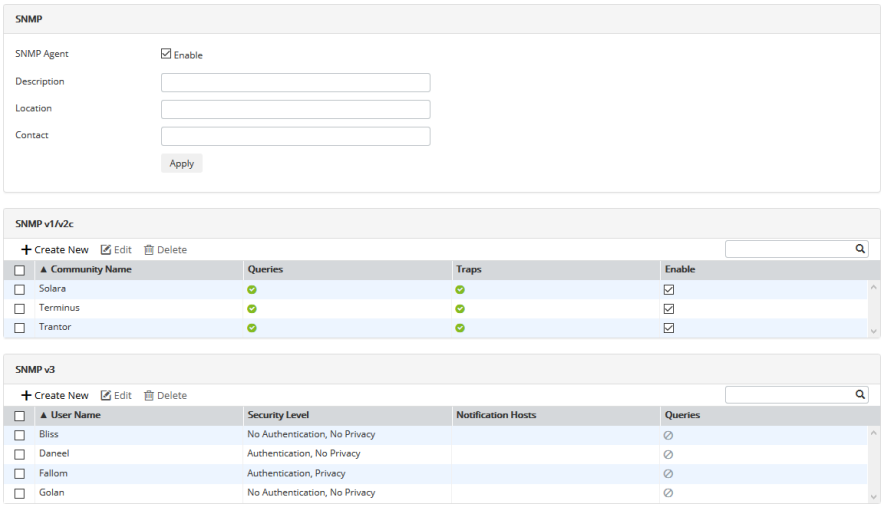
# SNMP

You can enable SNMP agent on FortiAnalyzer so that FortiAnalyzer can send traps to and receive queries from the computer that you designate as its SNMP manager. In this way, you can monitor your FortiAnalyzer with an SNMP manager.

## Configuring the SNMP agent

**To configure the FortiAnalyzer SNMP agent:**

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




2. Configure the following settings:

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

3. Configure SNMP v1/v2c communities. See Configuring SNMP v1/v2c communities on page 176.
4. Configure SNMP v3 users. See Configuring SNMP v3 users on page 178.

## Configuring SNMP v1/v2c communities

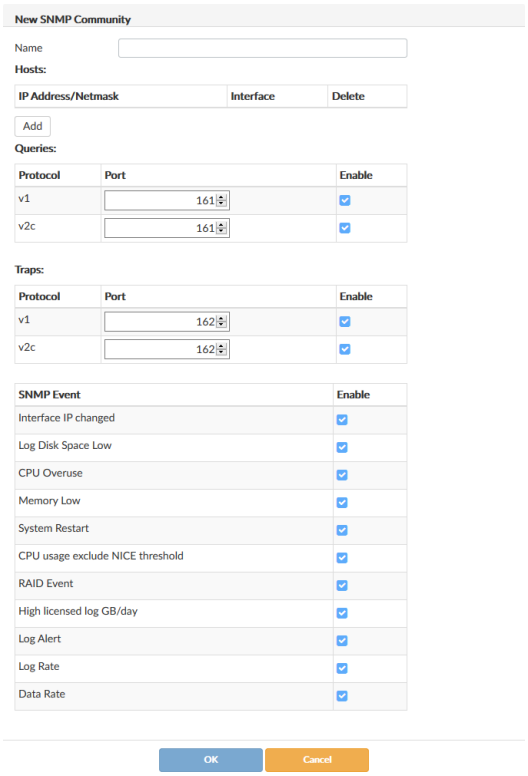
An SNMP community is a grouping of equipment for network administration purposes. You must configure your FortiAnalyzer to belong to at least one SNMP community so that community's SNMP managers can query the FortiAnalyzer system information and receive SNMP traps from it.

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.

**To add an SNMP community to the FortiAnalyzer SNMP agent:**

1. Go to the SNMP v1/v2c section of the SNMP page, and click *Create New*. The New SNMP Community pane is displayed.




2. Configure the following settings:

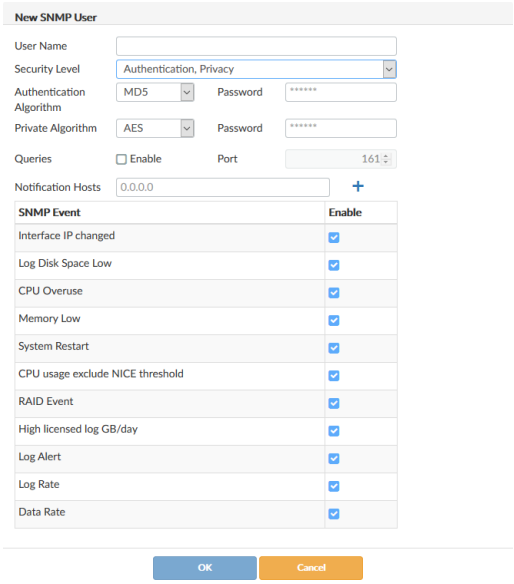
| | |
|---|---|
| **Name** | Type a name to identify the SNMP community. If you are editing an existing community, you will be unable to change the name. |

| | | |
|---|---|---|
| **Hosts** | | The list of hosts that can use the settings in this SNMP community to monitor the FortiAnalyzer system.<br><br>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. |
| | **IP Address** | Type the IP address of an SNMP manager. By default, the IP address is 0.0.0.0 so that any SNMP manager can use this SNMP community. |
| | **Interface** | Select the name of the interface that connects to the network where this SNMP manager is located from the drop-down list. You need to do this if the SNMP manager is on the Internet or behind a router. |
| | **Delete** | Select the delete icon to remove this SNMP manager entry. |
| | **Add** | Select to add a new default entry to the Hosts list that you can edit as needed. You can have up to eight SNMP manager entries for a single community. |
| **Queries** | | Type the port number (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 SNMP manager:<br>• Interface IP changed<br>• Log Disk Space Low<br>• CPU Overuse<br>• Memory Low<br>• System Restart<br>• CPU usage exclude NICE threshold<br>• RAID Event (only available for devices which support RAID)<br>• High licensed device quota<br>• High licensed log GB/day<br>• Log Alert<br>• Log Rate<br>• Data Rate |

## Configuring SNMP v3 users

**To add an SNMP v3 user:**

1. Go to the SNMP v3 section of the SNMP page, and click *Create New*. The New SNMP User pane is displayed.




2. Configure the following settings:

| | |
|---|---|
| **User Name** | The name of the SNMPv3 user. |
| **Security Level** | The security level of the user. Select one of the following:<br>• *No Authentication, No Privacy*<br>• *Authentication, No Privacy*: Select the authentication algorithm (SHA1, MD5) and enter the password.<br>• *Authentication, Privacy*: Select the authentication algorithm (SHA1, MD5), the private algorithm (AES, DES), and enter the password. |
| **Queries** | Select to enable queries then enter the port number. The default port is 161. |
| **Notification Hosts** | The IP address or addresses of the host. Click the add icon to add multiple IP addresses. |

| | |
|---|---|
| **SNMP Event** | Enable the events that will cause the FortiAnalyzer unit to send SNMP traps to the SNMP manager.<br>FortiAnalyzer SNMP events:<br>• Interface IP changed<br>• Log disk space low<br>• CPU Overuse<br>• Memory Low<br>• System Restart<br>• CPU usage exclude NICE threshold<br>• RAID Event (only available for devices which support RAID)<br>• High licensed device quota<br>• High licensed log GB/day<br>• Log Alert<br>• Log Rate<br>• Data Rate |

## SNMP MIBs

The Fortinet and FortiAnalyzer MIBs, along with the two RFC MIBs, can be obtained from Customer Service & Support (https://support.fortinet.com). You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib* MIB file in the firmware image file folder. The *FORTINET-CORE-MIB.mib* file is located in the main FortiAnalyzer 5.00 file folder.

To be able to communicate with the SNMP agent, you must include 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.

| MIB file name or RFC | Description |
|---|---|
| **FORTINET-CORE-MIB.mib** | The proprietary Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products.<br>Your SNMP manager requires this information to monitor Fortinet unit configuration settings and receive traps from the Fortinet SNMP agent. |
| **FORTINET-FORTIMANAGER-MIB.mib** | The proprietary FortiAnalyzer MIB includes system information and trap information for FortiAnalyzer units. |
| **RFC-1213 (MIB II)** | The Fortinet SNMP agent supports MIB II groups with the following exceptions.<br>• No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10).<br>• 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. |

| MIB file name or RFC | Description |
|---|---|
| **RFC-2665 (Ethernet-like MIB)** | The Fortinet SNMP agent supports Ethernet-like MIB information with the following exception.<br><br>No support for the dot3Tests and dot3Errors groups. |

## SNMP traps

Fortinet devices share SNMP traps, but each type of device also has traps specific to that device. For example 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. To view a trap or query's name, object identifier (OID), and description, open its MIB file in a plain text editor.

| Trap message | Description |
|---|---|
| **ColdStart, WarmStart, LinkUp, LinkDown** | Standard traps as described in RFC 1215. |
| **CPU usage high (fnTrapCpuThreshold)** | CPU usage exceeds the set percent. This threshold can be set in the CLI using the following commands:<br>`config system snmp sysinfo`<br>`  set trap-high-cpu-threshold <percentage value>`<br>`end` |
| **CPU usage excluding NICE processes (fmSysCpuUsageExcludedNice)** | CPU usage excluding NICE processes exceeds the set percentage. This threshold can be set in the CLI using the following commands:<br>`config system snmp sysinfo`<br>`  set trap-cpu-high-exclude-nice-threshold <percentage value>`<br>`end` |
| **Memory low (fnTrapMemThreshold)** | Memory usage exceeds 90 percent. This threshold can be set in the CLI using the following commands:<br>`config system snmp sysinfo`<br>`  set trap-low-memory-threshold <percentage value>`<br>`end` |
| **Log disk too full (fnTrapLogDiskThreshold)** | Log disk usage has exceeded the configured threshold. Only available on devices with log disks. |
| **Temperature too high (fnTrapTempHigh)** | A temperature sensor on the device has exceeded its threshold. Not all devices have thermal sensors. See manual for specifications. |

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

## 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 |
|---|---|
| **fnSysSerial** | Fortinet unit serial number. |

Administrator accounts:

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

Custom messages:

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

MIB fields and traps

| MIB field | Description |
|---|---|
| **fmModel** | A table of all FortiAnalyzer models. |

# Mail servers

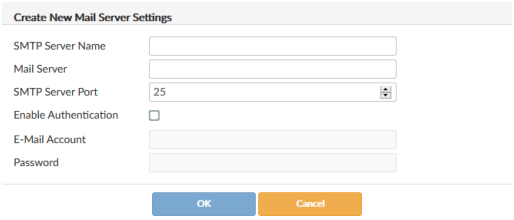
Go to System *Settings* > *Advanced* > *Mail Server* to configure SMTP mail server settings. Mail servers can be added, edited, deleted, and tested.

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.




Configure the following settings and then select *OK*:

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

**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*:

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

**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

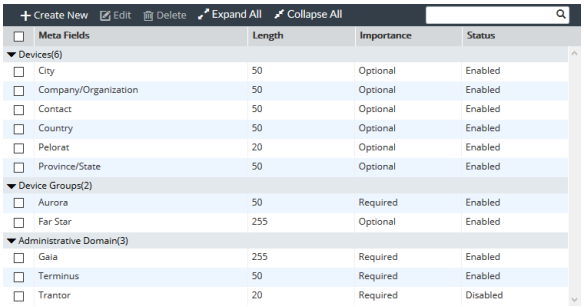
Meta fields allow administrators to add extra information when configuring, adding, or maintaining FortiGate units. You can make the fields mandatory or optional, and set the length of the field.

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. |




## 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:

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

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

# 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.

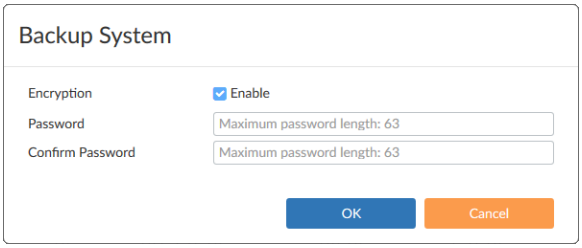
## Backing up the system configuration

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:

| | |
|---|---|
| **Choose Backup File** | Select *Browse...* to find the configuration backup file you want to restore on your management computer. |
| **Password** | Enter the encryption password, if applicable. |
| **Overwrite current IP, routing HA settings** | 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<br>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<br>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.<br>Protocol used will match the protocol used by the administrator when logging in to the GUI. | TCP 2032 |
| Log aggregation server<br>Log aggregation server support requires model FortiAnalyzer 800 series or greater. | TCP 3000 |
| Web Service | TCP 8080 |
| Ping | ICMP protocol |

FORTINET®

*High Performance Network Security*