FortiAnalyzer - Administration Guide

Version 5.6.9

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com/

FORTIGUARD CENTER
https://fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

July 25, 2019
FortiAnalyzer 5.6.9 Administration Guide
05-569-400231-20190725

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-07-18	Initial release.
2019-07-22	Added additional information to "Importing a log file" on page 122.
2019-07-25	Added Log Rate and Data Rate traps to "SNMP traps" on page 211.

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 Compatibility*
  This document identifies FortiAnalyzer software support for FortiOS.
- *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 Upgrade Guide*
  This document describes how to upgrade FortiAnalyzer.
- 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 VM Install Guide*
  This document describes installing FortiAnalyzer VM in your virtual environments.
- *FortiAnalyzer Administration Guide*
  This document describes how to set up the FortiAnalyzer system and use it with supported Fortinet units.
- *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 Dataset Reference*

  This document lists all of the datasets and macros available with FortiAnalyzer. Datasets and macros are used to create charts and reports in FortiAnalyzer.
- *FortiManager and FortiAnalyzer Event Log Reference*

  This document describes the log messages available with FortiAnalyzer when local logging is enabled.
- *FortiAnalyzer JSON API Reference*

  This document lists all of the objects available with the FortiAnalyzer JSON Application Programming Interface. The document is only available on the FNDN site at https://fndn.fortinet.net/.
- *FortiAnalyzer XML Reference*

  This document describes how to use the legacy XML-based FortiAnalyzer Application Programming Interface to obtain information from the FortiAnalyzer unit.

What's New in FortiAnalyzer

FortiAnalyzer version 5.6 includes the following new features and enhancements. Always review all sections in the *FortiAnalyzer Release Notes* prior to upgrading your device.

FortiAnalyzer 5.6.9

FortiAnalyzer 5.6.9 includes no new features.

FortiAnalyzer 5.6.8

FortiAnalyzer 5.6.8 includes no new features.

FortiAnalyzer 5.6.7

FortiAnalyzer 5.6.7 includes no new features.

FortiAnalyzer 5.6.6

FortiAnalyzer 5.6.6 includes the following new features and enhancements:

FortiView

Log ID for long sessions

In FortiView, *Log ID = 0000000020* indicates a long session that is not yet closed. A long session has multiple logs but is still considered one session. The sent/received data of long sessions counts all interim traffic data reported by lines with *Log ID = 0000000020*.

When the session is closed, the *Log ID* is *13*.

FortiAnalyzer 5.6.5

FortiAnalyzer 5.6.5 includes no new features.

FortiAnalyzer 5.6.4

FortiAnalyzer 5.6.4 includes no new features.

FortiAnalyzer 5.6.3

FortiAnalyzer 5.6.3 includes no new features.

FortiAnalyzer 5.6.2

FortiAnalyzer 5.6.2 includes the following new features and enhancements:

Improvements to Indicators of Compromise page

The *FortiView* > *Threats* > *Indicators of Compromise* page now provides a list of all the detected Indicators of Compromise by default. Through a new API, FortiAnalyzer can now share the Indicators of Compromise data with FortiOS. See FortiView Indicators of Compromise on page 103.

FortiAnalyzer 5.6.1

FortiAnalyzer 5.6.1 includes the following new features and enhancements:

Custom View Usability

In Log View, you can save new Custom Views directly from the menu bar, view log type for each saved Custom View, and apply a Custom View. See Custom views on page 118.

Configurable FortiGuard Server Location from System Settings

You can view the list of connected FortiGuard update servers from the *License Information* widget and update the list by selecting a preferred server location. See License Information widget on page 180.

FortiAnalyzer 5.6.0

FortiAnalyzer 5.6.0 includes the following new features and enhancements:

Fortinet Security Fabric

Security Fabric logging

- Store and analyze the logs from a Security Fabric as if they are from a *single* device. See What's new in your Security Fabric report on page 15.
- Support dynamic data and metadata exchange with Security Fabric.
- Synchronize the Security Fabric data and metadata from Collector to Analyzer. See Configuring Analyzer–Collector collaboration on page 30.
- Use the Security Fabric data in FortiView and Reports for additional visibility. See Report template library on page 156.

Endpoint Telemetry support

Use the endpoint telemetry data collected by the Security Fabric agent to display user profile photos in reports and FortiView. This provides more visibility for user identity. See Avatars on page 26 and Avatar on page 56.

Security Fabric logging topology

- Display logging topology of the entire Security Fabric for additional visibility.
- View the topology by device or by logging traffic.

See Displaying security fabric topology on page 84.

What's new in your Security Fabric report

Default report template for monitoring new users, devices, applications, vulnerabilities, threats, and so on from the Security Fabric. This report is in *Reports* > *Report Definitions* > *Templates* > *Template - What is New Report*.

Security Fabric Widgets

A set of dashboard widgets displays current audit scores for a FortiGate Security Fabric cluster with recommended best practices and the historical audit scores and trends. See NOC dashboards and widgets on page 109.

NOC/SOC Dashboard

- Purpose-designed dashboards for NOC/SOC operations.
- Enhanced visualization for real-time activities and historical trends for analysts to effectively monitor network activities and security alerts.

See NOC on page 106.

Log search

Log search performance has been improved.

Report templates

- GTP report template – new report template for FortiCarrier GTP traffic.
- DNS report template – new report template for DNS traffic.

See Report template library on page 156.

New DNS log

- Support for the new DNS log type introduced in FortiOS 5.6.
- DNS events are now logged with extra details in their own logs for better visibility,

See Datasets on page 165.

Near real-time logging

Provide flexibility for logs to be forwarded in more granular frequency such as every minute or every five minutes. See Log Forwarding on page 191.

JSON API

API support for Log View, FortiView, Reports, and Event Management. For more information, see the Fortinet Developer Network at https://fndn.fortinet.net/.

FortiClient EMS for Chromebooks support

FortiClient EMS for Chromebooks log support. See FortiClient support and ADOMs on page 44.

FortiAnalyzer-VM On-Demand for AWS

This release supports self-validated, on-demand instances of FortiAnalyzer-VM for AWS.

Key Concepts

This section provides information about basic FortiAnalyzer concepts and terms. If you are new to FortiAnalyzer, use this section to quickly understand this document and the FortiAnalyzer platform.

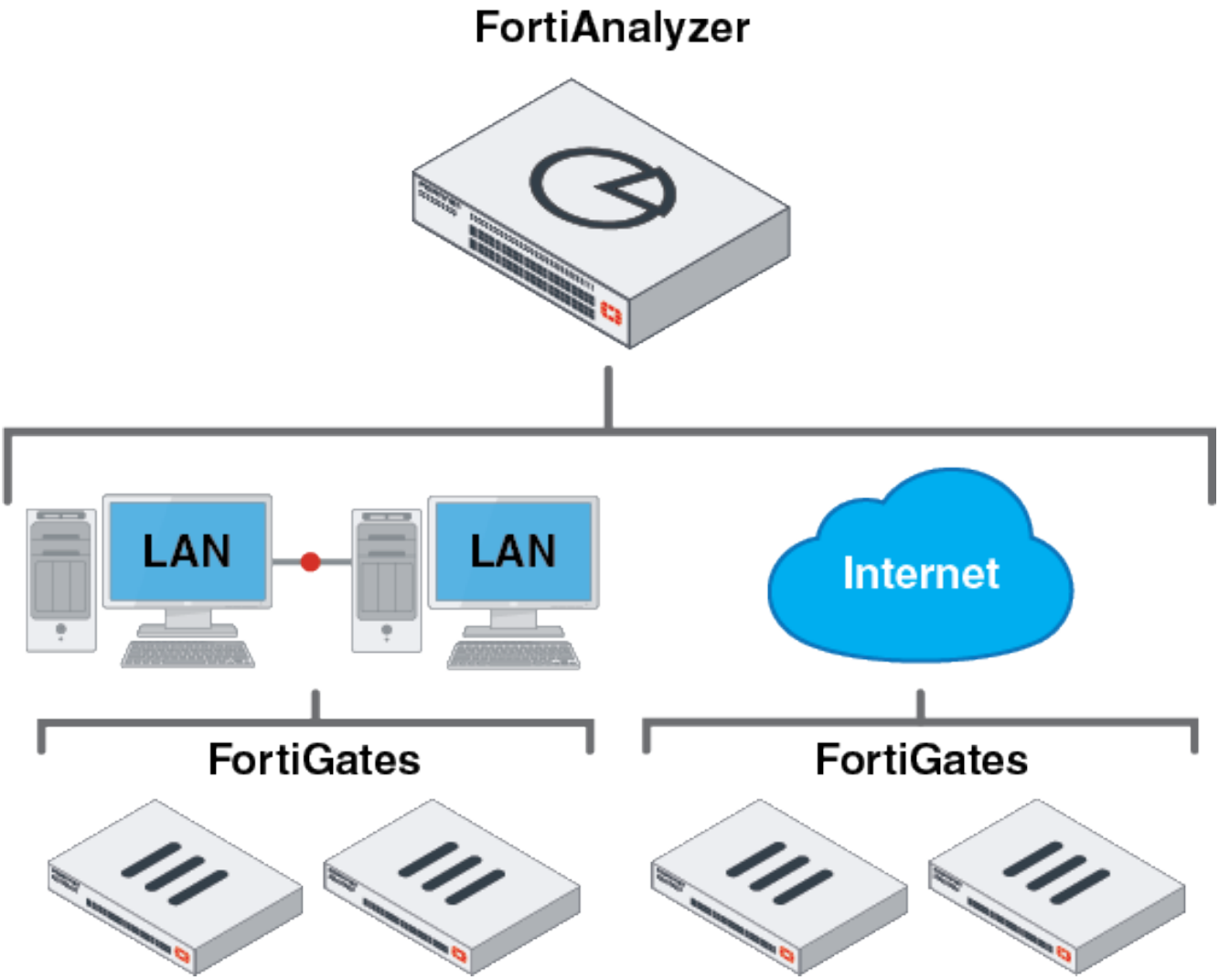
Two operation modes

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

Analyzer mode

Analyzer mode is the default mode that supports all FortiAnalyzer features. Use this mode to aggregate logs from one or more Collectors.

The following diagram shows an example of deploying FortiAnalyzer in Analyzer mode.



Collector mode

When FortiAnalyzer is in Collector mode, its primary task is forwarding logs of the connected devices to an Analyzer and archiving the logs. Instead of writing logs to the database, the Collector retains logs in their original binary format for uploading. In this mode, most features are disabled.

Analyzer and Collector feature comparison

Feature	Analyzer Mode	Collector Mode
Device Manager	Yes	Yes
FortiView	Yes	No

Feature	Analyzer Mode	Collector Mode
Log View	Yes	Raw archive logs only
Event Management	Yes	No
Monitoring devices	Yes	No
Reporting	Yes	No
System Settings	Yes	Yes
Log Forwarding	Yes	Yes

Analyzer–Collector collaboration

You can deploy 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 Analyzer offloads the log receiving task to the Collector so that the Analyzer can focus on data analysis and report generation. This maximizes the Collector's log receiving performance.

For an example of setting up Analyzer–Collector collaboration, see Configuring Analyzer–Collector collaboration on page 30.

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, the settings in your administrator account determines access to ADOMs.

For information on enabling and disabling ADOMs, see Enabling and disabling the ADOM feature on page 45. For information on working with ADOMs, see Administrative Domains on page 43. For information on configuring administrator accounts, See Managing administrator accounts on page 54.

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

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. These are collectively called log storage settings.

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

SQL database

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

For more information, see FortiView on page 93, Types of logs collected for each device on page 112, and Reports on page 141.

The log storage settings define how much FortiAnalyzer disk space to use for the SQL database.

The SQL database is disabled by default when FortiAnalyzer is in Collector mode so logs that require the SQL database are not available in Collector mode unless the SQL database is enabled. See Two operation modes on page 17.

Archive logs and Analytics logs

Logs in FortiAnalyzer are in one of the following phases. You can specify how long logs remain in each phase.

- Analytics logs: Indexed in the SQL database and online
- Archive logs: Compressed on hard disks and offline

In the indexed phase, logs are indexed in the SQL database for a specified length of time for the purpose of analysis. Logs in the indexed phase in the SQL database are considered online and you can view details about these logs in the *FortiView*, *Log View*, and *Event Management* pane. You can also generate reports about the logs in the *Reports* pane.

In the compressed phase, logs are compressed and archived in FortiAnalyzer disks for a specified length of time for the purpose of retention. Logs in the compressed phase are considered offline and you cannot immediately view details about these logs in the *FortiView*, *Log View*, and *Event Management* pane. You also cannot generate reports about the logs in the *Reports* pane.

Use a data policy to control how long to retain Archive and Analytics logs.

Data policy and automatic deletion

Use a data policy to control how long to keep compressed and indexed logs. When ADOMs are enabled, you can specify settings for each ADOM and the settings apply to all devices in that ADOM. When ADOMs are disabled, settings apply to all managed devices.

A data policy specifies:

- How long to keep Analytics logs indexed in the database
  When the specified length 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 length of time in the data policy expires, Archive logs are deleted from the FortiAnalyzer disks.

See also Log storage policy on page 89.

Disk utilization for Archive and Analytic 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.

Analytic logs indexed in the SQL database require more disk space than Archive logs (purged from the SQL database but remain compressed on the FortiAnalyzer disks). An average indexed log is 400 bytes and an average 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 settings for each ADOM and the settings apply to all devices in that ADOM. When ADOMs are disabled, settings apply to all managed devices. See Log storage policy on page 89.

Security Fabric

FortiAnalyzer can recognize a Security Fabric group of devices and display all units in the group on the *Device Manager* pane. See Adding a security fabric group on page 80. FortiAnalyzer supports the Security Fabric by storing and analyzing the logs from the units in a Security Fabric group as if the logs are from a single device. You can also view the logging topology of all units in the Security Fabric group for additional visibility. See Displaying security fabric topology on page 84.

FortiAnalyzer provides dynamic data and metadata exchange with the Security Fabric and uses the data in FortiView and Reports for additional visibility. A default report template lets you monitor new users, devices, applications, vulnerabilities, threats and so on from the Security Fabric.

A set of dashboard widgets lets you review audit scores for a FortiGate Security Fabric group with recommended best practices and historical audit scores and trends.

If FortiClient is installed on endpoints for endpoint control with FortiGate, you can use the endpoint telemetry data collected by the Security Fabric agent to display user profile photos in reports and FortiView.

NOC/SOC dashboard

FortiAnalyzer provides dashboard for Network Operations Center (NOC) or Security Operations Center (SOC) administrators. The dashboards enhance visualization for real-time activities and historical trends for analysts to effectively monitor network activities and security alerts. See NOC on page 106.

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

The FortiAnalyzer unit can be configured and managed using the GUI or the CLI. This section will step you through connecting to the unit via the GUI.

To connect to the GUI:

1. Connect the FortiAnalyzer unit to a management computer using an Ethernet cable.
2. Configure the management computer to be on the same subnet as the internal interface of the FortiAnalyzer unit:
   - IP address: 192.168.1.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 *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 FortiAnalyzer home page is displayed.
6. Click a tile to go to that pane. For example, click the *Device Manager* tile to go to the *Device Manager* 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.

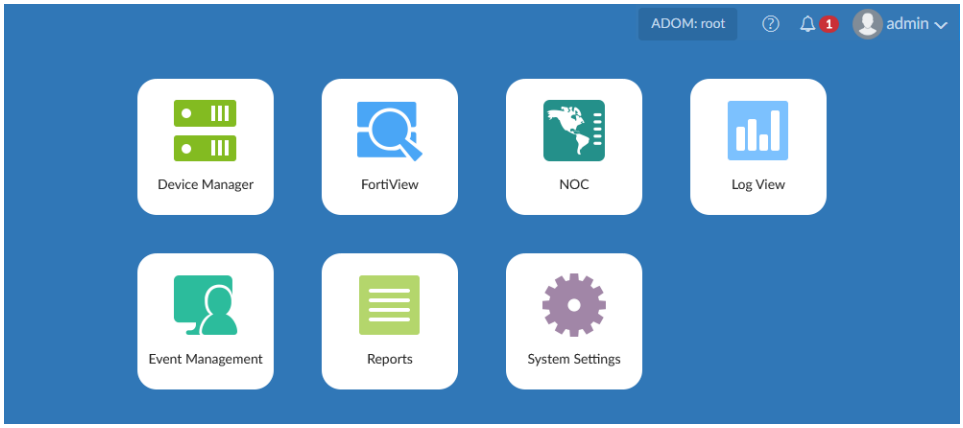
For information on enabling administrative access protocols and configuring IP addresses, see Configuring network interfaces on page 33.

If the URL is correct and you still cannot access the GUI, you may also need to configure static routes. For details, see Static routes on page 35.

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 Managing administrator accounts on page 54 for information.

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 Device Manager on page 77.
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. For each summary view, you can drill down into details for the event. See FortiView on page 93. This pane is not available when the unit is in Collector mode.
NOC	View network security, WiFi security, and system performance in real-time. You can select what activities to monitor in customizable dashboards. See NOC on page 106. This pane is not available when the unit is in Collector mode.
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 112.
Event Management	Configure and view events for logging devices. See Event Management on page 124. This pane is not available when the unit is in Collector mode.
Reports	Generate reports. You can also configure report templates, schedules, and output profiles, and manage charts and datasets. See Reports on page 141. This pane is not available when the unit is in Collector mode.
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 173.

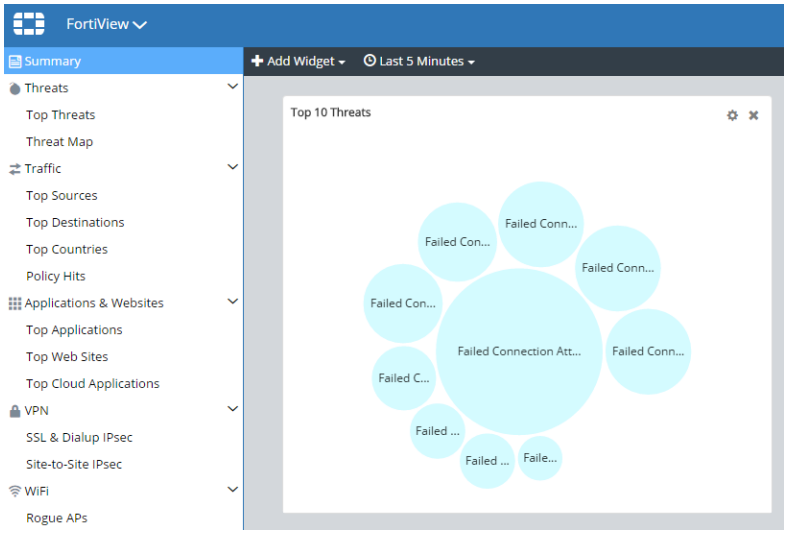
The top-right corner of the home page includes a variety of possible selections:

ADOM	If ADOMs are enabled, the required ADOM can be selected from the dropdown list. The ADOMs available from the ADOM menu will vary depending on the privileges of the current user.
Help	Click to open the FortiAnalyzer online help, or view the *About* information for your device (Product, Version, and Build Number). You can also open the FortiAnalyzer basic setup video (https://video.fortinet.com/video/208/fortianalyzer-basic-setup).
Notification	Click to display a list of notifications. Select a notification from the list to take action on the issue.
admin	Click to change the password or log out of the GUI.

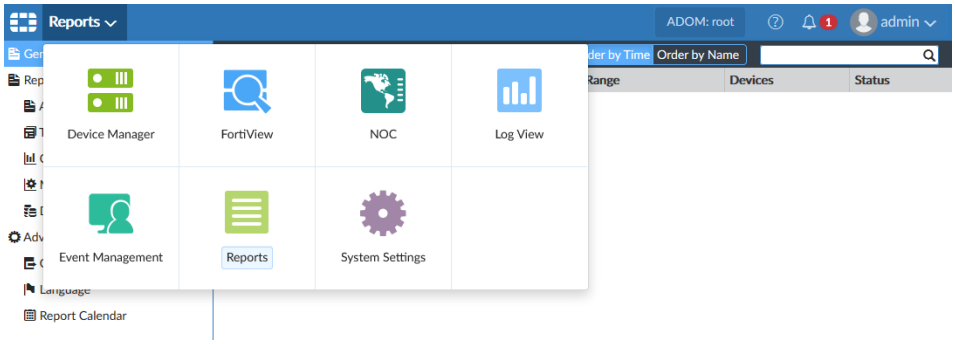
Panes

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.



Color themes

You can choose a color theme for the FortiAnalyzer GUI. For example, you can choose a color, such as blue or plum, or you can choose an image, such as summer or autumn. See Global administration settings on page 69.

Full-screen mode

You can view several panes in full-screen mode. When a pane is in full-screen mode, tree menu on the left side of the screen is hidden.

Click the *Full Screen* button in the toolbar to enter full-screen mode, and press the *Esc* key on your keyboard to exit full-screen mode.

Switching between ADOMs

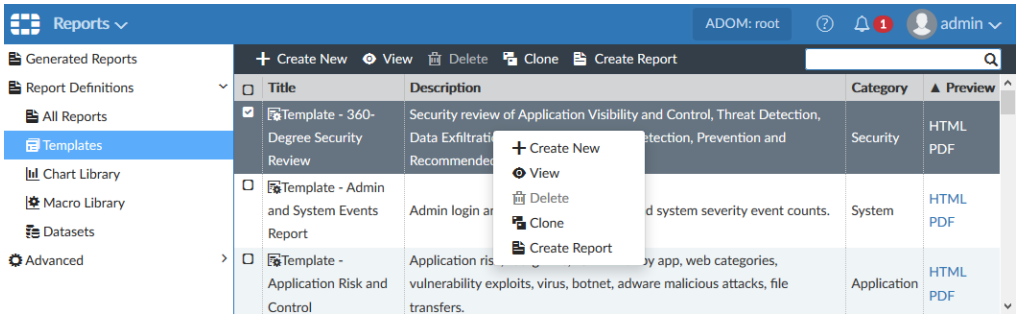
When ADOMs are enabled, you can move between ADOMs by selecting an ADOM from the *ADOM* menu in the banner.

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 Managing administrator accounts on page 54 for more information.

Using the right-click menu

Options are sometimes available using the right-click menu. Right-click an item in the content pane, or within some of the tree menus, to display the menu that includes various options similar to those available in the toolbar.

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



Avatars

When FortiClient sends logs to FortiAnalyzer, an avatar for each user can be displayed in the *Source* column in the *FortiView* and *Log View* panes. FortiAnalyzer can display an avatar when the following requirements are met:

- FortiClient is managed by FortiGate or FortiClient EMS with logging to FortiAnalyzer enabled.
- FortiClient sends logs and a picture of each user to FortiAnalyzer.

If FortiAnalyzer cannot find the defined picture, a generic, gray avatar is displayed.

You can also optionally define an avatar for FortiAnalyzer administrators. See Creating administrators on page 55.

Showing and hiding passwords

In some cases you can show and hide passwords by using the toggle icon. When you can view the password, the *Toggle show password* icon is displayed:

When you can hide the password, the *Toggle hide password* icon is displayed:

Security considerations

You can take steps to prevent unauthorized access and restrict access to the GUI.

Restricting GUI access by trusted host

To prevent unauthorized access to the GUI you can configure administrator accounts with trusted hosts. With trusted hosts configured, the administrator user can only log into the GUI when working on a computer with the trusted host as defined in the administrator account. You can configure up to ten trusted hosts per administrator account. See Administrators on page 53 for more details.

Other security considerations

Other security consideration for restricting access to the FortiAnalyzer GUI include the following:

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

Restarting and shutting down

Always use the operation options in the GUI or the CLI commands to reboot 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. Enter *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. Enter `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. Enter `y` to continue. The device will reset to factory default settings and restart.

To reset logs and re-transfer all SQL logs to 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. Enter `y` to continue. All SQL logs will be resent to 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 58.

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 the RAID level on page 39.
3. Configure network settings. See Configuring network interfaces on page 33.

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 Managing ADOMs on page 46.
5. Configure administrator accounts. See Managing administrator accounts on page 54.

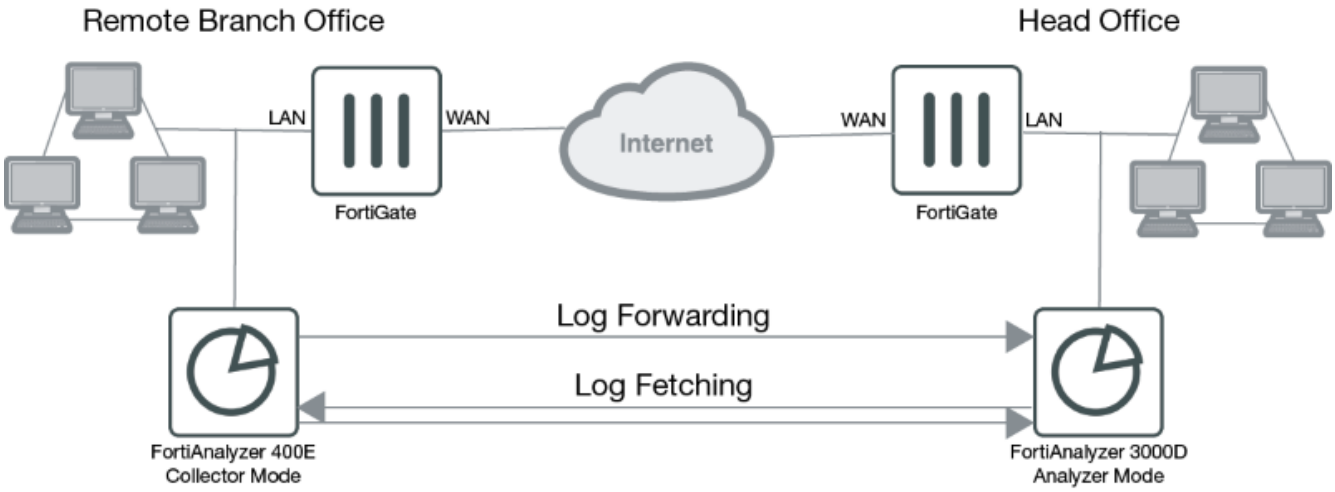
After you configure the administrator accounts for the FortiAnalyzer unit, you should log in again by using your new administrator account.

6. Add devices to the FortiAnalyzer unit so that the devices can send logs to the FortiAnalyzer unit. See Adding devices on page 78.

7. Configure the operation mode. See Configuring the operation mode on page 180 and Two operation modes on page 17.

Configuring Analyzer–Collector collaboration

This topic describes how to configure two FortiAnalyzer units as the Analyzer and Collector and make them work together. In the scenario shown in the diagram below, Company A has a remote branch network with a FortiGate unit and a FortiAnalyzer 400E in Collector mode. In its head office, Company A has another FortiGate unit and a FortiAnalyzer 3000D in Analyzer mode. 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 is also used for log archival.



For related concepts, see Two operation modes on page 17 and Analyzer–Collector collaboration on page 19. You need to complete the initial setup for your FortiAnalyzer units first. See Initial setup on page 29.

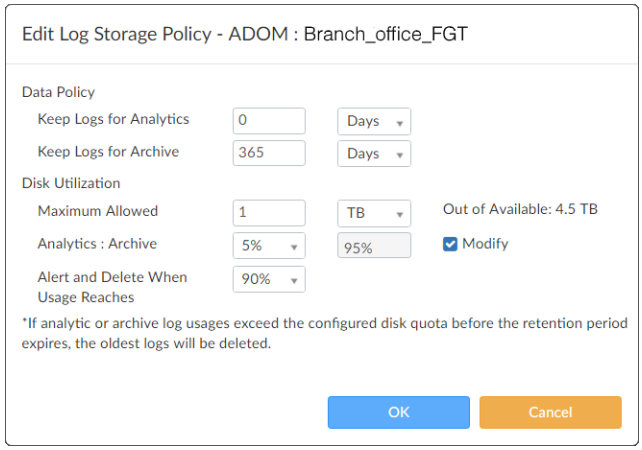
Configuring the Collector

To configure the Collector:

1. Ensure the FortiAnalyzer Operation Mode is *Collector*. See Configuring the operation mode on page 180.
2. Check and configure the storage policy for the Collector. See Log storage policy on page 89.

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 191. 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.

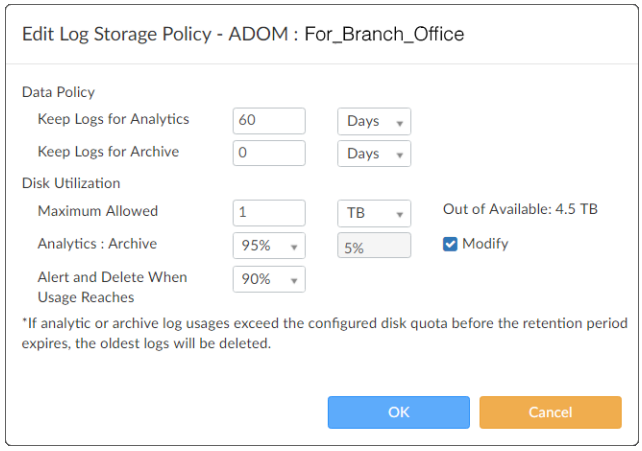
Configuring the Analyzer

To configure the Analyzer:

1. Ensure the FortiAnalyzer Operation Mode is *Analyzer*. See Configuring the operation mode on page 180
2. Check and configure the storage policy for the Analyzer. See Log storage policy on page 89.

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 log-forward-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 80.

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 Fetcher Management on page 195.

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 Types of logs collected for each device on page 112.
- View summaries of threats, traffic, and more in *FortiView*. See FortiView on page 93
- View multiple panes of network activity in NOC (Network Operations Center) or SOC (Security Operations Center). See NOC on page 106.
- Generate and view events in *Event Management*. See Event Management on page 124.
- Generate and view reports in *Reports*. See Reports on page 141.

Network

The network settings are used to configure ports for the FortiAnalyzer unit. You should also specify what port and methods that an administrators can use to access the FortiAnalyzer unit. If required, static routes can be configured.

The default port for FortiAnalyzer units is port 1. It can be used to configure one IP address for the FortiAnalyzer unit, or multiple ports can be configured with multiple IP addresses for improved security.

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

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 53 and Managing administrator accounts on page 54.

Configuring network interfaces

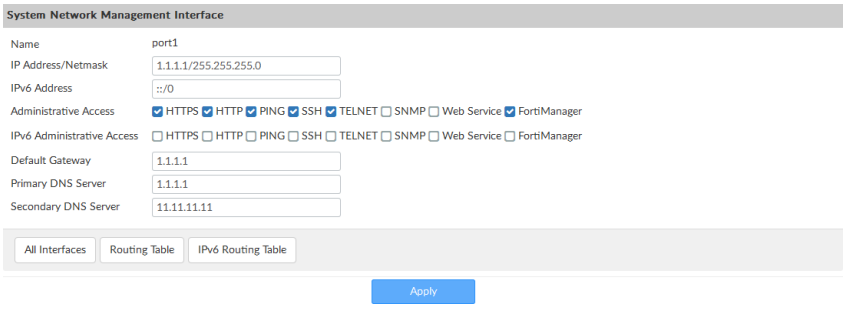
Fortinet devices can be connected to any of the FortiAnalyzer unit's interfaces. The DNS servers must be on the networks to which the FortiAnalyzer unit connects, and should have two different IP addresses.

The following port configuration is recommended:

- Use port1 for device log traffic, and disable unneeded services on it, 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.

To configured port 1:

1. Go to *System Settings* > *Network*. The *System Network Management Interface* pane is displayed.



2. Configure the following settings for *port1*, then click *Apply* to apply your changes.

Name	Displays the name of the interface.
IP Address/Netmask	The IP address and netmask associated with this interface.

IPv6 Address	The IPv6 address associated with this interface.
Administrative Access	Select the allowed administrative service protocols from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, 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	The default gateway associated with this interface.
Primary DNS Server	The primary DNS server IP address.
Secondary DNS Server	The secondary DNS server IP address.

To configure additional ports:

1. Go to *System Settings* > *Network* and click *All Interfaces*. The interface list opens.
2. Double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. Configure the settings as required.
4. Click *OK* to apply your changes.

The port name, default gateway, and DNS servers cannot be changed from the *Edit System Interface* pane. The port can be given an alias if needed.

Disabling ports

Ports can be disabled to prevent them from accepting network traffic

To disable a port:

1. Go to *System Settings* > *Network* and click *All Interfaces*. The interface list opens.
2. Double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. In the *Status* field, click *Disable*
4. Click *OK* to disable the port.

Changing administrative access

Administrative access defines the protocols that can be used to connect to the FortiAnalyzer through an interface. The available options are: HTTPS, HTTP, PING, SSH, TELNET, SNMP, Web Service, and FortiManager.

To change administrative access:

1. Go to *System Settings* > *Network* and click *All Interfaces*. The interface list opens.
2. Double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. Select one or more access protocols for the interface for IPv4 and IPv6, if applicable.
4. Click *OK* to apply your changes.

Static routes

Static routes can managed from the routing tables for IPv4 and IPv6 routes.

The routing tables can be accessed by going to *System Settings* > *Network* and clicking *Routing Table* and *IPv6 Routing Table*.

To add a static route:

1. From the IPv4 or IPv6 routing table, click *Create New* in the toolbar. The *Create New Network Route* pane opens.
2. Enter the destination IP address and netmask, or IPv6 prefix, and gateway in the requisite fields.
3. Select the network interface that connects to the gateway from the dropdown list.
4. Click *OK* to create the new static route.

To edit a static route:

1. From the IPv4 or IPv6 routing table: double-click on a route, right-click on a route then select *Edit* from the pop-up menu, or select a route then click *Edit* in the toolbar. The *Edit Network Route* pane opens.
2. Edit the configuration as required. The route ID cannot be changed.
3. Click *OK* to apply your changes.

To delete a static route or routes:

1. From the IPv4 or IPv6 routing table, right-click on a route then select *Delete* from the pop-up menu, or select a route or routes then click *Delete* in the toolbar.
2. Click *OK* in the confirmation dialog box to delete the selected route or routes.

RAID Management

RAID helps to divide data storage over multiple disks, providing increased data reliability. For FortiAnalyzer devices containing multiple hard disks, you can configure the RAID array for capacity, performance, and/or availability.

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:

See the FortiAnalyzer datasheet to determine your devices supported RAID levels.

Linear RAID

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

RAID 0

A RAID 0 array is also referred to as striping. The 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 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 1s

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

RAID 5

A RAID 5 array employs striping with a parity check. Similar to RAID 0, the 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 5s

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

RAID 6

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

- Minimum number of drives: 4
- Data protection: Up to two disk failures.

RAID 6s

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:

- 2 RAID 1 arrays of two disks each,
- 3 RAID 1 arrays of two disks each,
- 6 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.

Configuring the RAID level

Changing the RAID level will delete all data.

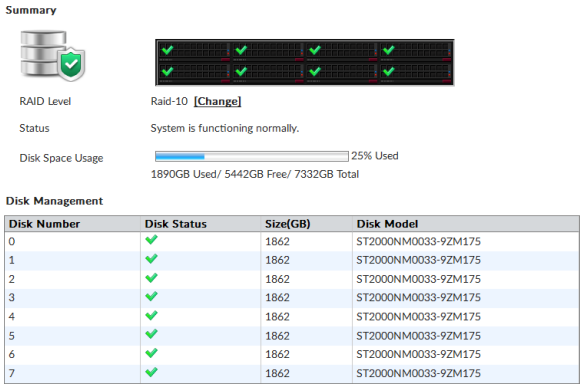
To configure the RAID level:

1. Go to *System Settings* > *RAID Management*.
2. Click *Change* in the *RAID Level* field. The *RAID Settings* dialog box is displayed.
3. From the *RAID Level* list, select a new RAID level, then 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.

Monitoring RAID status

To view the RAID status, go to *System Settings* > *RAID Management*. The RAID Management pane displays the RAID level, status, and disk space usage. It also shows the status, size, and model of each disk in the RAID array.

The *Alert Message Console* widget, located in *System Settings* > *Dashboard*, provides detailed information about RAID array failures. For more information see Alert Messages Console widget on page 182.



Summary		Shows summary information about the RAID array.
	Graphic	Displays the position and status of each disk in the RAID array. Hover the cursor over each disk to view 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.

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	Shows information about each disk in the RAID array.
Disk Number	Identifies the disk number for each disk.
Disk Status	Displays the status of each disk in the RAID array. • *Ready*: The hard drive is functioning normally. • *Rebuilding*: The FortiAnalyzer unit is writing data to a newly added hard drive in order to restore the hard drive to an optimal state. The FortiAnalyzer unit is not fully fault tolerant until rebuilding is complete. • *Initializing*: The FortiAnalyzer unit is writing to all the hard drives in the device in order to make the array fault tolerant. • *Verifying*: The FortiAnalyzer unit is ensuring that the parity data of a redundant drive is valid. • *Degraded*: The hard drive is no longer being used by the RAID controller. • *Inoperable*: One or more drives are missing from the FortiAnalyzer unit. The drive is no longer available to the operating system. Data on an inoperable drive cannot be accessed.
Size (GB)	Displays the size, in GB, of each disk.
Disk Model	Displays the model number of each disk.

Checking RAID from command line

Use command line to check if your device uses hardware or software RAID.

To check RAID type from the command line:

1. Go to *System Settings*.
2. Click *CLI Console*.
3. Type the command `diagnose system raid status` and press *Enter*.
4. The following information is shown in the output:
   - Mega RAID - this output shows that the device uses hardware RAID.
   - Software RAID - this output shows that the device uses software RAID.

Sample command line output showing RAID:

```
[Product_Name_Model] # diagnose system raid status
   Mega RAID: <-- this is hardware RAID
   RAID Level: Raid-50
   RAID Status: OK
   RAID Size: 11175GB
   Groups: 2
```

```
[Product_Name_Model] # diagnose system raid status
   Software RAID: <-- this is software RAID
   RAID Level: Raid-50
   RAID Status: OK
   RAID Size: 11175GB
   Groups: 2
```

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 unit is still running - known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

To identify which hard disk failed, read the relevant log message in the *Alert Message Console* widget. See Alert Messages Console widget on page 182.

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 is 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:

1. Remove the faulty hard disk.
2. Install a new disk.

   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 checkmark icon for all disks and the *RAID Status* area displays the progress of the RAID re-synchronization/rebuild.

Adding hard disks

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

Fortinet recommends 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 the risk of data loss.
3. Install the disks in the FortiAnalyzer unit.
   If your unit supports hot swapping, you can do so while the unit is running. Otherwise the unit must be shut down first. See Unit Operation widget on page 181 for information.
4. Configure the RAID level. See Configuring the RAID level on page 39.
5. If you backed up the log data, restore it.

Administrative Domains

Administrative domains (ADOMs) enable administrators to manage only those devices that they are specifically assigned, based on the ADOMs to which they have access. When the ADOM mode is advanced, FortiGate devices with multiple VDOMs can be divided among multiple ADOMs.

Administrator accounts can be tied to one or more ADOMs, or denied access to specific ADOMs. When a particular administrator logs in, they see only those devices or VDOMs that have been enabled for their account. Super user administrator accounts, such as the `admin` account, can see and maintain all ADOMs and the devices within them.

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

The maximum number of ADOMs you can add depends on the FortiAnalyzer system model. Please refer to the FortiAnalyzer data sheet for more information.

By default, ADOMs are disabled. Enabling and configuring ADOMs can only be done by administrators with the *Super_User* profile. See Administrators on page 53.

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

ADOMs must be enabled to support the logging and reporting of non-FortiGate devices.

Default ADOMs

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

For example, when you add a FortiClient EMS device to the 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 selectable 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* pane.

Organizing devices into ADOMs

You can organize devices into ADOMs to allow you to better manage these devices. Devices can be organized by whatever method you deem appropriate, for example:

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

FortiClient support and ADOMs

FortiClient logs are stored in the device that the FortiClient endpoint is registered to.

For example, when endpoints are registered to a FortiGate device, FortiClient logs are viewed on the FortiGate device. When endpoints are registered to a FortiClient EMS, FortiClient logs are viewed in the FortiClient ADOM that the FortiClient EMS device is added to.

ADOMs must be enabled to support FortiClient EMS devices.

Merge FortiAnalyzer Logging Support for FortiClient EMS for Chromebooks

1. Add `http-logging` and `https-logging` to the `allowaccess` list using the following CLI command:
```
config system interface
   edit "port1"
      set allowaccess https ssh http http-logging https-logging
   next
end
```
2. Add SSL certificate to enable communication.

   An SSL certificate is required to support communication and send logs between FortiClient Web Filter extension and FortiAnalyzer. If you use a public SSL certificate, you only need to add the public SSL certificate to FortiAnalyzer.

   However, if you prefer to use a certificate that is not from a common CA, you must add the SSL certificate to FortiAnalyzer, and you must push the root CA of your certificate to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient EMS Chromebook Web Filter extension and FortiAnalyzer will not work. The common name of the certificate must be the FortiAnalyzer IP address.

   a. In FortiAnalyzer, go to *System Settings* > *Certificates* > *Local Certificates*.
   b. Click *Import*. The *Import Local Certificate* dialog box appears.
   c. In the *Type* list, select *Certificate*. Or,
      In the *Type* list, select *PKCS#12 Certificate* to upload the certificate in PK12 format.
   d. Beside the *Certificate File* field, click *Browse* to select the certificate.
   e. Enter the *password* and *certificate name*.
   f. Click *OK*.

3. Select certificates for HTTPS connections:
   a. In FortiAnalyzer, go to *System Settings* > *Admin* > *Admin Settings*.
   b. In the *HTTPS & Web Service Certificate* box, select the certificate you want to use for HTTPS connections, and click *Apply*.
4. Enable the FortiClient ADOM using the following CLI command:
```
conf sys global
   set adom-status enable
end
```
5. Add FortiClient EMS for Chromebooks as a device to the FortiClient ADOM:
   Go to *Device Manager* > *click the + Add Device button* to add FortiClient EMS for Chromebooks as a FortiClient ADOM device.
6. Enable logging in FortiClient EMS for Chromebooks:
   You will need to enable logging in FortiClient EMS for Chromebooks, see the *FortiClient EMS for Chromebooks Administration Guide* for more information.

Enabling and disabling the ADOM feature

By default, ADOMs are disabled. Enabling and configuring ADOMs can only be done by super user administrators.

When ADOMs are enabled, the *Device Manager*, *FortiView*, *Log View*, *Event Management*, and *Reports* panes are displayed per ADOM. You select the ADOM you need to work in when you log into the FortiAnalyzer unit. Switching between ADOMs on page 25.

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

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

To enable the ADOM feature:

1. Log in to the FortiAnalyzer as a super user administrator.
2. Go to *System Settings* > *Dashboard*.
3. In the *System Information* widget, toggle the *Administrative Domain* switch to *ON*.
   You will be automatically logged out of the FortiAnalyzer and returned to the log in screen.

To disable the ADOM feature:

1. Remove all the devices from all non-root ADOMs. That is, add all devices to the root ADOM.
2. Delete all non-root ADOMs. See Deleting ADOMs on page 51.
   Only after removing all the non-root ADOMs can ADOMs be disabled.
3. Go to *System Settings* > *Dashboard*.

4. In the *System Information* widget, toggle the *Administrative Domain* switch to *OFF*.
   You will be automatically logged out of the FortiAnalyzer and returned to the log in screen.

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

ADOM device modes

An ADOM has two device modes: *Normal* (default) and *Advanced*.

In *Normal* mode, you cannot assign different FortiGate VDOMs to different ADOMs. The FortiGate unit can only be added to a single ADOM.

In *Advanced* mode, you can assign a VDOM from a single device to a different ADOM (ADOM cannot be in backup mode). This allows you to analyze data for individual VDOMs, but will result in more complicated management scenarios. It is recommended only for advanced users.

To change from *Advanced* mode back to *Normal* mode, you must ensure no FortiGate VDOMs are assigned to an ADOM.

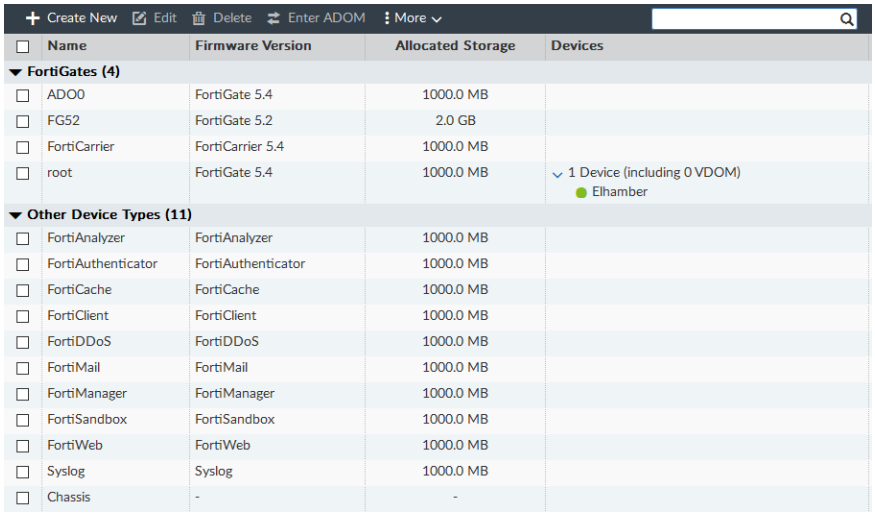
To change the ADOM device mode:

1. Go to *System Settings* > *Advanced* > *Advanced Settings*.
2. In the ADOM Mode field, select either *Normal* or *Advanced*.
3. Select *Apply* to apply your changes.

Managing ADOMs

The ADOMs feature must be enabled before ADOMs can be created or configured. See Enabling and disabling the ADOM feature on page 45.

To create and manage ADOMs, go to *System Settings* > *All ADOMs*.



Create New	Create a new ADOM. See Creating ADOMs on page 48.
Edit	Edit the selected ADOM. This option is also available from the right-click menu. See Editing an ADOM on page 51.
Delete	Delete the selected ADOM or ADOMs. You cannot delete default ADOMs. This option is also available from the right-click menu. See Deleting ADOMs on page 51.
Enter ADOM	Switch to the selected ADOM. This option is also available from the right-click menu.
More	Select *Expand Devices* to expand all of the ADOMs to show the devices in each ADOM. Select *Collapse Devices* to collapses the device lists. These options are also available from the right-click menu.
Search	Enter a search term to search the ADOM list.
Name	The name of the ADOM. ADOMs are listed in the following groups: *FortiGates* and *Other Device Types*. A group can be collapsed or expanded by clicking the triangle next to its name.
Firmware Version	The version is only displayed if FortiManager features are enabled. The firmware version of the ADOM. Devices in the ADOM should have the same firmware version.
Allocated Storage	The amount of hard drive storage space allocated to the ADOM.
Devices	The number of devices and VDOMs that the ADOM contains. The device list can be expanded or by clicking the triangle.

Creating ADOMs

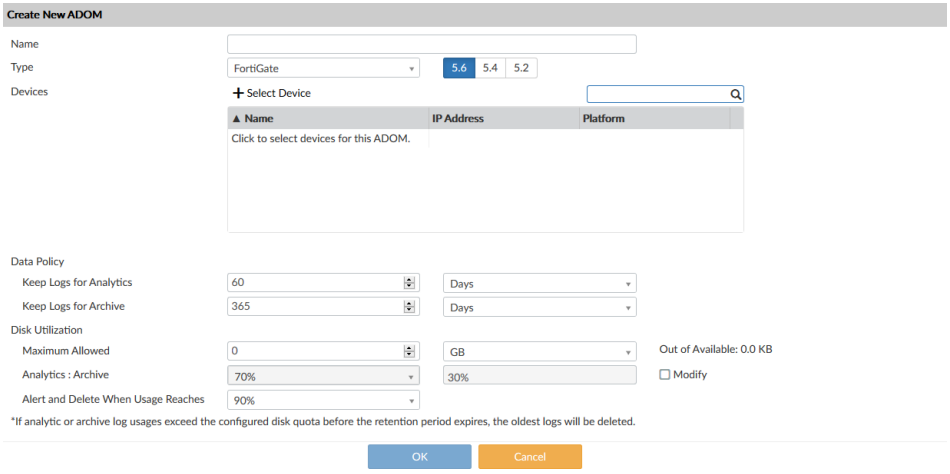
To create a new ADOM, you must be logged in as a super user administrator.

Consider the following when creating ADOMs:

- The maximum number of ADOMs that can be created depends on the FortiAnalyzer model. For more information, see the FortiAnalyzer data sheet at https://www.fortinet.com/products/management/fortianalyzer.html.
- You must use an administrator account that is assigned the *Super_User* administrative profile.
- You can 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 advanced device mode. See ADOM device modes on page 46.
- You can configure how an ADOM handles log files from its devices. For example, you can configure how much disk space an ADOM can use for logs, and then monitor how much of the allotted disk space is used. You can also specify how long to keep logs in the SQL database and how long to keep logs stored in compressed format.

To create an ADOM

1. Ensure that ADOMs are enabled. See Enabling and disabling the ADOM feature on page 45.
2. Go to *System Settings* > *All ADOMs*.
3. Click *Create New* in the toolbar. The *Create New ADOM* pane is displayed.



4. Configure the following settings, then click *OK* to create the ADOM.

Name	Type a name that allows you to distinguish this ADOM from your other ADOMs. ADOM names must be unique.
Type	Select the type of device that you are creating an ADOM for. The ADOM type cannot be edited. Although you can create a different ADOM for each type of device, FortiAnalyzer does not enforce this setting.

Version	 Version is only available if FortiManager features are enabled and the device type is FortiGate or FortiCarrier. Select the version of the devices in the ADOM. The ADOM version cannot be edited. Although you can create a different ADOM for each version, FortiAnalyzer does not enforce this setting.
Devices	Add a device or devices with the selected versions to the ADOM. The search field can be used to find specific devices. See Assigning devices to an ADOM on page 50.
Data Policy	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. Information about the logs can be viewed in the *FortiView*, *Event Management*, and *Reports* modules. After the specified length of time expires, Analytics 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, information about the log messages cannot be viewed in the *FortiView*, *Event Management*, or *Reports* modules. After the specified length of time expires, Archive logs are automatically deleted from the FortiAnalyzer unit.
Disk Utilization	Specify how much disk space to use for logs.
Maximum Allowed	Specify the maximum amount of FortiAnalyzer disk space to use for logs, and select the unit of measure. The total available space on the FortiAnalyzer unit is shown. For more info about the maximum available space for each FortiAnalyzer unit, see Disk space allocation on page 86.
Analytics : Archive	Specify the percentage 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* checkbox to change the setting.
Alert and Delete When Usage Reaches	Specify at what data usage percentage an alert messages will be generated and logs will be automatically deleted. The oldest Archive log files or Analytics database tables are deleted first.

Assigning devices to an ADOM

To assign devices to an ADOM you must be logged in as a super user administrator. Devices cannot be assigned to multiple ADOMs.

To assign devices to an ADOM:

1. Go to *System Settings* > *All ADOMs*.
2. Double-click on an ADOM, right-click on an ADOM and then select the *Edit* from the menu, or select the ADOM then click *Edit* in the toolbar. The *Edit ADOM* pane opens.
3. Click *Select Device*. The *Select Device* list opens on the right side of the screen.
4. Select the devices that you want to add to the ADOM. Only devices with the same version as the ADOM can be added. The selected devices are displayed in the *Devices* list.

   If the ADOM mode is *Advanced* you can add separate VDOMs to the ADOM as well as units.
5. When done selecting devices, click *Close* to close the *Select Device* list.
6. Click *OK*.

   The selected devices are removed from their previous ADOM and added to this one.

Assigning VDOMs to an ADOM

To assign VDOMs to an ADOM you must be logged in as a super user administrator and the ADOM mode must be *Advanced* (see ADOM device modes on page 46). VDOMs cannot be assigned to multiple ADOMs.

To assign VDOMs to an ADOM:

1. Go to *System Settings* > *All ADOMs*.
2. Double-click on an ADOM, right-click on an ADOM and then select the *Edit* from the menu, or select the ADOM then click *Edit* in the toolbar. The *Edit ADOM* pane opens.
3. Click *Select Device*. The *Select Device* list opens on the right side of the screen.
4. Select the VDOMs that you want to add to the ADOM. Only VDOMs on devices with the same version as the ADOM can be added. The selected VDOMs are displayed in the *Devices* list.
5. When done selecting VDOMs, click *Close* to close the *Select Device* list.
6. Click *OK*.

   The selected VDOMs are removed from their previous ADOM and added to this one.

Assigning administrators to an ADOM

Super user administrators can create other administrators and either assign ADOMs to their account or exclude them from specific ADOMs, constraining them to configurations and data that apply only to devices in the ADOMs they can access.

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 48.

To assign an administrator to specific ADOMs:

1. Log in as a super user administrator. Other types of administrators cannot configure administrator accounts when ADOMs are enabled.
2. Go to *System Settings* > *Admin* > *Administrator*.
3. Double-click on an administrator, right-click on an administrator and then select the *Edit* from the menu, or select the administrator then click *Edit* in the toolbar. The *Edit Administrator* pane opens.
4. Edit the *Administrative Domain* field as required, either assigning or excluding specific ADOMs.
5. Select *OK* to apply your changes.

The *admin* administrator account cannot be restricted to specific ADOMs.

Editing an ADOM

To edit an ADOM you must be logged in as a super user administrator. The ADOM type and version cannot be edited. For the default ADOMs, the name cannot be edited.

To edit an ADOM:

1. Go to *System Settings* > *All ADOMs*.
2. Double-click on an ADOM, right-click on an ADOM and then select *Edit* from the menu, or select the ADOM then click *Edit* in the toolbar. The *Edit ADOM* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

Deleting ADOMs

To delete an ADOM, you must be logged in as a super-user administrator (see Administrator profiles on page 58), such as the *admin* administrator.

Prior to deleting an ADOM:

- All devices must be removed from the ADOM. Devices can be moved to another ADOM, or to the root ADOM. See Assigning devices to an ADOM on page 50.
- References to the ADOM must be removed from administrator accounts (or the accounts deleted). See Assigning administrators to an ADOM on page 50.

To delete an ADOM:

1. Go to *System Settings* > *All ADOMs*.
2. Ensure that the ADOM or ADOMs being deleted have no devices in them.
3. Select the ADOM or ADOMs you need to delete.
4. Click *Delete* in the toolbar, or right-click and select *Delete*.
5. Click *OK* in the confirmation box to delete the ADOM or ADOMs.

Default ADOMs cannot be deleted.

Administrators

The *System Settings* > *Admin* menu enables you to configure administrator accounts, access profiles, remote authentication servers, and adjust global administrative settings for the FortiAnalyzer unit.

Administrator accounts are used to control access to the FortiAnalyzer unit. Local and remote authentication is supported, as well as two-factor authentication. Administrator profiles define different types of administrators and the level of access they have to the FortiAnalyzer unit, as well as the devices registered to it.

Global administration settings, such as the GUI language and password policies, can be configured on the *Admin Settings* pane. See Global administration settings on page 69 for more information.

Trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative permissions. 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 to both 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.

Monitoring administrators

The *Admin Session List* lets you view a list of administrators currently logged in to the FortiAnalyzer unit.

To view logged in administrators:

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

   The following information is available:

User Name	The name of the administrator account. Your session is indicated by *(current)*.

IP Address	The IP address where the administrator is logging in from. This field also displays the logon type (GUI, jsconsole, SSH, or telnet).
Start Time	The date and time the administrator logged in.
Time Out (mins)	The maximum duration of the session in minutes (1 to 480 minutes).

Disconnecting administrators

Administrators can be disconnected from the FortiAnalyzer unit from the *Admin Session List*.

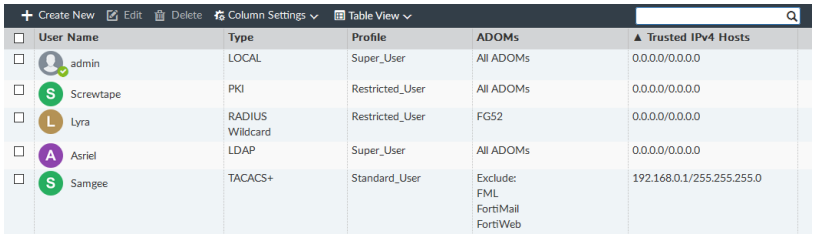
To disconnect administrators:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Current Administrators* field, click the *Current Session List* button. The *Admin Session List* opens in the widget.
3. Select the administrator or administrators you need to disconnect.
4. Click *Delete* in the toolbar, or right-click and select *Delete*.
   The selected administrators will be automatically disconnected from the FortiAnalyzer device.

Managing administrator accounts

Go to *System Settings* > *Admin* > *Administrator* to view the list of administrators and manage administrator accounts.

Only administrators with the *Super_User* profile can see the complete administrators list. If you do not have certain viewing permissions, you will not see the administrator list. When ADOMs are enabled, administrators can only access the ADOMs they have permission to access.



The following options are available:

Create New	Create a new administrator. See Creating administrators on page 55.
Edit	Edit the selected administrator. See Editing administrators on page 57.
Delete	Delete the selected administrator or administrators. See Deleting administrators on page 58.
Column Settings	Change the displayed columns.

Table View/Tile View	Change the view of the administrator list. Table view shows a list of the administrators in a table format. Tile view shows a separate card for each administrator in a grid pattern.
Search	Search the administrators.
Change Password	Change the selected administrator's password. This option is only available from the right-click menu. See Editing administrators on page 57.

The following information is shown:

User Name	The name the administrator uses to log in.
Type	The user type, as well as if the administrator uses a wildcard.
Profile	The profile applied to the administrator. See Administrator profiles on page 58
ADOMs	The ADOMs the administrator has access to or is excluded from.
Comments	Comments about the administrator account. This column is hidden by default.
Email	The contact email associated with the administrator. This column is hidden by default.
Phone	The contact phone number associated with the administrator. This column is hidden by default.
Trusted IPv4 Hosts	The IPv4 trusted host(s) associated with the administrator. See Trusted hosts on page 53.
Trusted IPv6 Hosts	The IPv6 trusted host(s) associated with the administrator. See Trusted hosts on page 53. This column is hidden by default.

Creating administrators

To create a new administrator account, you must be logged in to an account with sufficient privileges, or as a super user administrator.

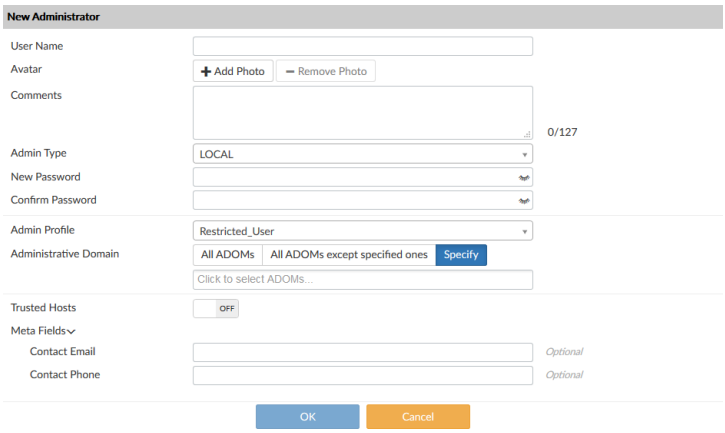
You need the following information to create an account:

- Which authentication method the administrator will use to log in to the FortiAnalyzer unit. Local, remote, and Public Key Infrastructure (PKI) authentication methods are supported.
- What administrator profile the account will be assigned, or what system privileges the account requires.
- If ADOMs are enabled, which ADOMs the administrator will require access to.
- If using trusted hosts, the trusted host addresses and network masks.

For remote or PKI authentication, the authentication must be configured before you create the administrator. See Authentication on page 62 for details.

To create a new administrator:

1. Go to *System Settings* > *Admin* > *Administrators*.
2. Click *Create New* in the toolbar. The *New Administrator* pane opens.



3. Configure the following settings, and then click *OK* to create the new administrator.

User Name	Enter the name the administrator will use to log in.
Avatar	Apply a custom image to the administrator. Click *Add Photo* to select an image already loaded to the FortiAnalyzer, or to load an new image from the management computer. If no image is selected, the avatar will use the first letter of the user name.
Comments	Optionally, enter a description of the administrator, such as their role, location, or the reason for their account.
Admin Type	Select the type of authentication the administrator will use when logging into the FortiAnalyzer unit. One of: *LOCAL*, *RADIUS*, *LDAP*, *TACACS+*, *PKI*, or *Group*. See Authentication on page 62 for more information.
Server or Group	Select the RADIUS server, LDAP server, TACACS+ server, or group, as required. The server must be configured prior to creating the new administrator. This option is not available if the *Admin Type* is *LOCAL* or *PKI*.
Wildcard	Select this option to set the password as a wildcard. This option is not available if the *Admin Type* is *LOCAL* or *PKI*.
Subject	Enter a comment for the PKI administrator. This option is only available if the *Admin Type* is *PKI*.
CA	Select the CA certificate from the dropdown list. This option is only available if the *Admin Type* is *PKI*.
Required two-factor authentication	Select to enable two-factor authentication. This option is only available if the *Admin Type* is *PKI*.

New Password	Enter the password. This option is not available if *Wildcard* is selected. If the *Admin Type* is *PKI*, this option is only available when *Require two-factor authentication* is selected. If the *Admin Type* is *RADIUS*, *LDAP*, or *TACACS+*, the password is only used when the remote server is unreachable.
Confirm Password	Enter the password again to confirm it. This option is not available if *Wildcard* is selected. If the *Admin Type* is *PKI*, this option is only available when *Require two-factor authentication* is selected.
Admin Profile	Select an administrator profile from the list. The profile selected determines the administrator's access to the FortiAnalyzer unit's features. See Administrator profiles on page 58.
Administrative Domain	Choose the ADOMs this administrator will be able to access. • *All ADOMs*: The administrator can access all the ADOMs. • *All ADOMs except specified ones*: The administrator cannot access the selected ADOMs. • *Specify*: The administrator can access the selected ADOMs. If the *Admin Profile* is *Super_User*, then the setting is *All ADOMs*. This field is available only if ADOMs are enabled. See Administrative Domains on page 43.
Trusted Hosts	Optionally, turn on trusted hosts, then enter their IP addresses and netmasks. Up to ten IPv4 and ten IPv6 hosts can be added. See Trusted hosts on page 53 for more information.
Meta Fields	Optionally, enter the new administrator's email address and phone number.

Editing administrators

To edit an administrator, you must be logged in as a super user administrator. The administrator's name cannot be edited. An administrator's password can be changed using the right-click menu, if the password is not a wildcard.

To edit an administrator:

1. Go to *System Settings* > *Admin* > *Administrators*.
2. Double-click on an administrator, right-click on an administrator and then select *Edit* from the menu, or select the administrator then click *Edit* in the toolbar. The *Edit Administrator* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

To change an administrator's password:

1. Go to *System Settings* > *Admin* > *Administrators*.
2. Right-click on an administrator and select *Change Password* from the menu. The *Change Password* dialog box opens.

3. If you are editing the *admin* administrator's password, enter the old password in the *Old Password* field.
4. Enter the new password for the administrator in the *New Password* and *Confirm Password* fields.
5. Select *OK* to change the administrator's password.

The current administrator's password can also be changed from the admin menu in the GUI banner. See GUI on page 22 for information.

Deleting administrators

To delete an administrator or administrators, you must be logged in as a super user administrator.

You cannot delete an administrator that is currently logged in to the device.

The *admin* administrator can only be deleted using the CLI.

To delete an administrator or administrators:

1. Go to *System Settings* > *Admin* > *Administrators*.
2. Select the administrator or administrators you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the administrator or administrators.

To delete an administrator using the CLI:

1. Open a CLI console and enter the following command:

```
config system admin user
   delete <username>
end
```

Administrator profiles

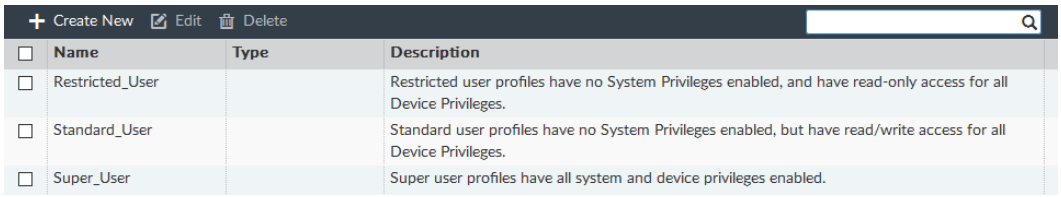
Administrator profiles are used to control administrator access privileges to devices or system features. Profiles are assigned to administrator accounts when an administrator is created. The profile controls access to both the FortiAnalyzer GUI and CLI.

There are three predefined system profiles:

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, and have read/write access for all device privileges.
Super_User	Super user profiles have all system and device privileges enabled. It cannot be edited.

These profiles cannot be deleted, but standard and restricted profiles can be edited. New profiles can also be created as required. Only super user administrators can manage administrator profiles.

Go to *System Settings* > *Admin* > *Profile* to view and manage administrator profiles.



The following options are available:

Create New	Create a new administrator profile. See Creating administrator profiles on page 60.
Edit	Edit the selected profile. See Editing administrator profiles on page 61.
Delete	Delete the selected profile or profiles. See Deleting administrator profiles on page 61.
Search	Search the administrator profiles list.

The following information is shown:

Name	The name the administrator uses to log in.
Type	The profile type.
Description	A description of the system and device access permissions allowed for the selected profile.

Permissions

The below table lists the default permissions for the predefined administrator profiles.

When *Read-Write* is selected, the user can view and make changes to the FortiAnalyzer system. When *Read-Only* is selected, the user can only view information. When *None* is selected, the user can neither view or make changes to the FortiAnalyzer system.

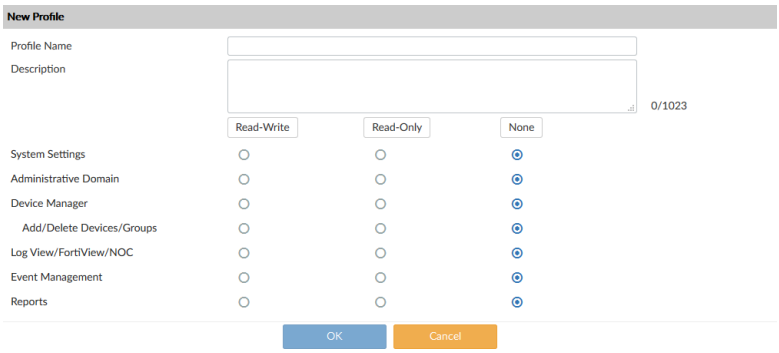
Setting	Predefined Administrator Profile		
	Super User	Standard User	Restricted User
System Settings `system-setting`	Read-Write	None	None
Administrative Domain `adom-switch`	Read-Write	Read-Write	None
Device Manager `device-manager`	Read-Write	Read-Write	Read-Only
Add/Delete Devices/Groups `device-op`	Read-Write	Read-Write	None
Log View/FortiView/NOC `log-viewer`	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			
`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
`device-fortiswitch`	Read-Write	Read-Write	Read-Only
`realtime-monitor`	Read-Write	Read-Write	Read-Only

Creating administrator profiles

To create a new administrator profile, you must be logged in to an account with sufficient privileges, or as a super user administrator.

To create a custom administrator profile:

1. Go to *System Settings* > *Admin* > *Profile*.
2. Click *Create New* in the toolbar. The *New Profile* pane is displayed.



3. Configure the following settings, and then click *OK* to create the new administrator profile.

Profile Name	Enter a name for this profile.
Description	Optionally, 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.
Permissions	Select *None*, *Read Only*, or *Read-Write* access for the categories as required.

Editing administrator profiles

To edit an administrator profile, you must be logged in to an account with sufficient privileges, or as a super user administrator. The profile's name cannot be edited. The *Super_User* profile cannot be edited, and the predefined profiles cannot be delete.

To edit an administrator:

1. Go to *System Settings* > *Admin* > *Profile*.
2. Double-click on a profile, right-click on a profile and then select *Edit* from the menu, or select the profile then click *Edit* in the toolbar. The *Edit Profile* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

Deleting administrator profiles

To delete a profile or profiles, you must be logged in to an account with sufficient privileges, or as a super user administrator. The predefined profiles cannot be deleted.

To delete a profile or profiles:

1. Go to *System Settings* > *Admin* > *Profile*.
2. Select the profile or profiles you need to delete.

3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the profile or profiles.

Authentication

The FortiAnalyzer system supports authentication of administrators locally, remotely with RADIUS, LDAP, or TACACS+ servers, and using PKI. Remote authentication servers can also be added to authentication groups that administrators can use for authentication.

To use PKI authentication, you must configure the authentication before you create the administrator accounts. See Public Key Infrastructure on page 62 for more information.

To use remote authentication servers, you must configure the appropriate server entries in the FortiAnalyzer unit for each authentication server in your network. New LDAP remote authentication servers can be added and linked to all ADOMs or specific ADOMs. See LDAP servers on page 65, RADIUS servers on page 66, and TACACS+ servers on page 67 for more information.

Public Key Infrastructure

Public Key Infrastructure (PKI) authentication uses X.509 certificate authentication library that takes a list of peers, peer groups, and user groups and returns authentication successful or denied notifications. Administrators only need a valid X.509 certificate for successful authentication; no username or password is necessary.

To use PKI authentication for an administrator, you must configure the authentication before you create the administrator accounts. You will also need the following certificates:

- an X.509 certificate for the FortiManager administrator (administrator certificate)
- an X.509 certificate from the Certificate Authority (CA) which has signed the administrator's certificate (CA Certificate)

To get the CA certificate:

1. Log into your FortiAuthenticator.
2. Go to *Certificate Management* > *Certificate Authorities* > *Local CAs*.
3. Select the certificate and select *Export* in the toolbar to save the `ca_fortinet.com` CA certificate to your management computer. The saved CA certificate's filename is `ca_fortinet.com.crt`.

To get the administrator certificate:

1. Log into your FortiAuthenticator.
2. Go to *Certificate Management* > *End Entities* > *Users*.
3. Select the certificate and select *Export* in the toolbar to save the administrator certificate to your management computer. The saved CA certificate's filename is `admin_fortinet.com.p12`. This PCKS#12 file is password protected. You must enter a password on export.

To import the administrator certificate into your browser:

1. In Mozilla Firefox, go to *Options* > *Advanced* > *Certificates* > *View Certificates* > *Import*.
2. Select the file `admin_fortinet.com.p12` and enter the password used in the previous step.

To import the CA certificate into the FortiAnalyzer:

1. Log into your FortiAnalyzer.
2. Go to *System Settings* > *Certificates* > *CA Certificates*.
3. Click *Import*, and browse for the `ca_fortinet.com.crt` file you saved to your management computer, or drag and drop the file onto the dialog box. The certificate is displayed as *CA_Cert_1*.

To create a new PKI administrator account:

1. Go to *System Settings* > *Admin* > *Administrator*.
2. Click *Create New*. The *New Administrator* dialog box opens.
   See Creating administrators on page 55 for more information.
3. Select *PKI* for the *Admin Type*.
4. Enter a comment in the *Subject* field for the PKI administrator.
5. Select the CA certificate from the dropdown list in the *CA* field.
6. Click *OK* to create the new administrator account.

PKI authentication must be enabled via the FortiAnalyzer CLI with the following commands:

```
config system global
set clt-cert-reg enable
end
```

When connecting to the FortiAnalyzer GUI, you must use HTTPS when using PKI certificate authentication.

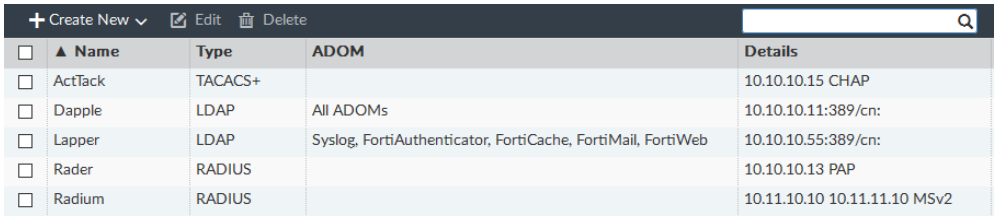
When both `set clt-cert-req` and `set admin-https-pki-required` are enabled, only PKI administrators can connect to the FortiAnalyzer GUI.

Managing remote authentication servers

The FortiAnalyzer system supports remote authentication of administrators using LDAP, RADIUS, and TACACS+ remote servers. To use this feature, you must configure the appropriate server entries for each authentication server in your network, see LDAP servers on page 65, RADIUS servers on page 66, and TACACS+ servers on page 67 for more information.

Remote authentication servers can be added, edited, deleted, and added to authentication groups (CLI only).

Go to *System Settings* > *Admin* > *Remote Authentication Server* to manage remote authentication servers.



The following options are available:

Create New	Add an LDAP, RADIUS, or TACACS+ remote authentication server. See LDAP servers on page 65, RADIUS servers on page 66, and TACACS+ servers on page 67.
Edit	Edit the selected remote authentication server. See Editing remote authentication servers on page 64.
Delete	Delete the selected remote authentication server or servers. See Deleting remote authentication servers on page 64.

The following information is displayed:

Name	The name of the server.
Type	The server type: *LDAP*, *RADIUS*, or *TACACS+*.
ADOM	The administrative domain(s) which are linked to the remote authentication server.
Details	Details about the server, such as the IP address.

Editing remote authentication servers

To edit a remote authentication server, you must be logged in to an account with sufficient privileges, or as a super user administrator. The server's name cannot be edited.

To edit a remote authentication server:

1. Go to *System Settings* > *Admin* > *Remote Authentication Server*.
2. Double-click on a server, right-click on a server and then select *Edit* from the menu, or select the server then click *Edit* in the toolbar. The *Edit Server* pane for that server type opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

   See LDAP servers on page 65, RADIUS servers on page 66, and TACACS+ servers on page 67 for more information.

Deleting remote authentication servers

To delete a remote authentication server or servers, you must be logged in to an account with sufficient privileges, or as a super user administrator.

To delete a remote authentication server or servers:

1. Go to *System Settings* > *Admin* > *Remote Authentication Server*.
2. Select the server or servers you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the server or servers.

LDAP servers

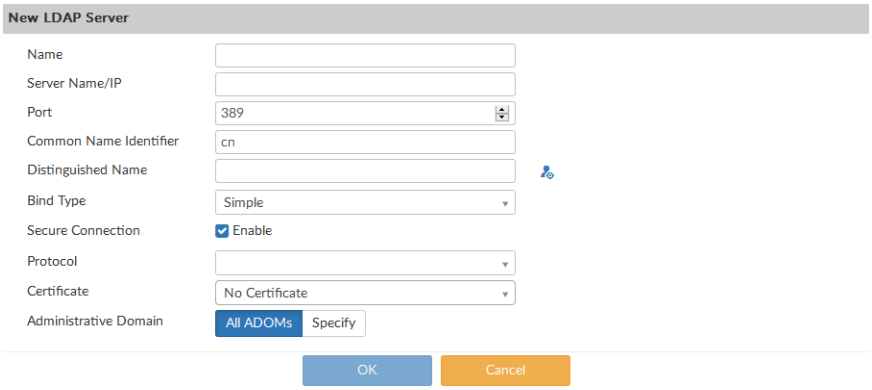
Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request/response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

If you have configured LDAP support and an administrator is required to authenticate using an LDAP server, the FortiAnalyzer unit sends the administrator's credentials to the LDAP server for authentication. If the LDAP server can authenticate the administrator, they are successfully authenticated with the FortiAnalyzer unit. If the LDAP server cannot authenticate the administrator, the FortiAnalyzer unit refuses the connection.

To use an LDAP server to authenticate administrators, you must configure the server before configuring the administrator accounts that will use it.

To add an LDAP server:

1. Go to *System Settings* > *Admin* > *Remote Authentication Server*.
2. Select *Create New* > *LDAP Server* from the toolbar. The *New LDAP Server* pane opens.



3. Configure the following settings, and then click *OK* to add the LDAP server.

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 is used to look up entries on the LDAP server. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. Clicking the *query distinguished name* icon will query the LDAP server for the name and open the *LDAP Distinguished Name Query* window to display the results.
Bind Type	Select the type of binding for LDAP authentication: *Simple*, *Anonymous*, or *Regular*.
User DN	When the *Bind Type* is set to *Regular*, enter the user DN.
Password	When the *Bind Type* is set to *Regular*, enter the password.
Secure Connection	Select to use a secure LDAP server connection for authentication.
Protocol	When *Secure Connection* is enabled, select either LDAPS or STARTTLS.
Certificate	When *Secure Connection* is enabled, select the certificate from the dropdown list.
Administrative Domain	Choose the ADOMs that this server will be linked to for reporting: *All ADOMs* (default), or *Specify* for specific ADOMs.

RADIUS servers

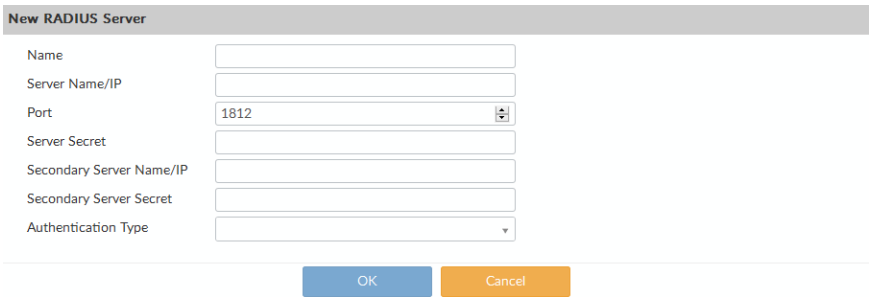
Remote Authentication Dial-in User (RADIUS) is a user authentication and network-usage accounting system. When users connect to a server they type a user name and password. This information is passed to a RADIUS server, which authenticates the user and authorizes access to the network.

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

To use a RADIUS server to authenticate administrators, you must configure the server before configuring the administrator accounts that will use it.

To add a RADIUS server:

1. Go to *System Settings* > *Admin* > *Remote Authentication Server*.
2. Select *Create New* > *RADIUS Server* from the toolbar. The *New RADIUS Server* pane opens.



3. Configure the following settings, and then click *OK* to add the RADIUS server.

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	Select the authentication type the RADIUS server requires. If you select the default *ANY*, FortiAnalyzer tries all authentication types.

TACACS+ servers

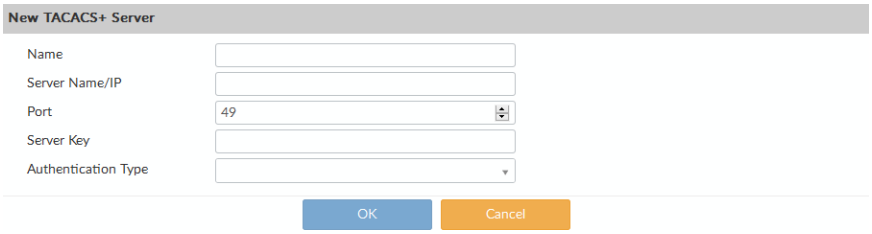
Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other network computing devices via one or more centralized servers. It allows a client to accept a user name and password and send a query 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.

If you have configured TACACS+ support and an administrator is required to authenticate using a TACACS+ server, the FortiAnalyzer unit contacts the TACACS+ server for authentication. If the TACACS+ server can authenticate the administrator, they are successfully authenticated with the FortiAnalyzer unit. If the TACACS+ server cannot authenticate the administrator, the connection is refused by the FortiAnalyzer unit.

To use a TACACS+ server to authenticate administrators, you must configure the server before configuring the administrator accounts that will use it.

To add a TACACS+ server:

1. Go to *System Settings* > *Admin* > *Remote Authentication Server*.
2. Select *Create New* > *TACACS+ Server* from the toolbar. The *New TACACS+ Server* pane opens.



3. Configure the following settings, and then click *OK* to add the TACACS+ server.

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	Select the authentication type the TACACS+ server requires. If you select the default *ANY*, FortiAnalyzer tries all authentication types.

Remote authentication server groups

Remote authentication server groups can be used to extend wildcard administrator access. Normally, a wildcard administrator can only be created for a single server. If multiple servers of different types are grouped, a wildcard administrator can be applied to all of the servers in the group.

Multiple servers of the same type can be grouped to act as backups - if one server fails, the administrator can still be authenticated by another server in the group.

To use a server group to authenticate administrators, you must configure the group before configuring the administrator accounts that will use it.

Remote authentication server groups can only be managed using the CLI. For more information, see the *FortiAnalyzer CLI Reference*.

To create a new remote authentication server group:

1. Open the admin group command shell:
```
config system admin group
```
2. Create a new group, or edit an already create group:
```
edit <group name>
```
3. Add remote authentication servers to the group:
```
set member <server name> <server name> ...
```
4. Apply your changes:
```
end
```

To edit the servers in a group:

1. Enter the following CLI commands:
```
config system admin group
   edit <group name>
         set member <server name> <server name> ...
   end
```
Only the servers listed in the command will be in the group.

To remove all the servers from the group:

1. Enter the following CLI commands:
```
config system admin group
   edit <group name>
      unset member
   end
```
All of the servers in the group will be removed.

To delete a group:

1. Enter the following CLI commands:
```
config system admin group
   delete <group name>
end
```

Global administration settings

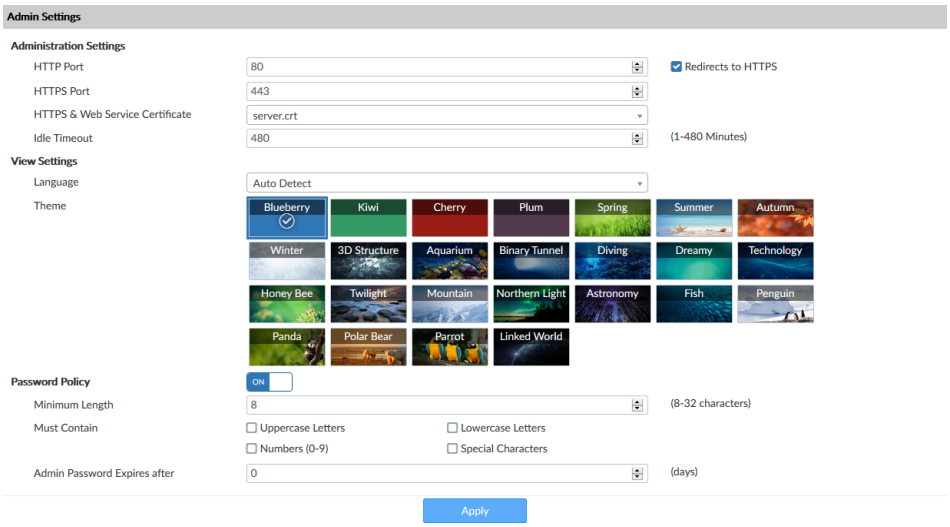
The administration settings page provides options for configuring global settings for administrator access to the FortiAnalyzer device. Settings include:

- Ports for HTTPS and HTTP administrative access
  To improve security, you can change the default port configurations for administrative connections to the FortiAnalyzer. When connecting to the FortiAnalyzer unit when the port has changed, the port must be included, such as `https://<ip_address>:<port>`. For example, if you are connecting to the FortiAnalyzer unit using port 8080, the URL would be `https://192.168.1.99:8080`. When you change to the default port number for HTTP, HTTPS, Telnet, or SSH, ensure that the port number is unique.
- Idle timeout settings
  By default, the GUI disconnects administrative sessions if no activity occurs for five minutes. This prevents someone from using the GUI if the management computer is left unattended.
- GUI language
  The language the GUI uses. For best results, you should select the language used by the management computer.
- GUI theme
  The default color theme of the GUI is *Blueberry*. You can choose another color or an image.
- Password policy
  Enforce password policies for administrators.

Only super user administrators can access and configure the administration settings. The settings are global and apply to all administrators of the FortiAnalyzer unit.

To configure the administration settings:

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



2. Configure the following settings as needed, then click *Apply* to save your changes to all administrator accounts:

Administration Settings		
	HTTP Port	Enter the TCP port to be used for administrative HTTP access. Default: 80. Select *Redirect to HTTPS* to redirect HTTP traffic to HTTPS.
	HTTPS Port	Enter the TCP port to be used for administrative HTTPS access. Default: 443.
	HTTPS & Web Service Server Certificate	Select a certificate from the dropdown list.
	Idle Timeout	Enter the number of minutes an administrative connection can be idle before the administrator must log in again, from 1 to 480 (8 hours). See Idle timeout on page 72 for more information.
View Settings		
	Language	Select a language from the dropdown list. See GUI language on page 72 for more information.
	Theme	Select a theme for the GUI. The selected theme is not applied until you click *Apply*, allowing to you to sample different themes. Default: Blueberry.
Password Policy		Click to enable administrator password policies. See Password policy on page 71 and Password lockout and retry attempts on page 71 for more information.
	Minimum Length	Select the minimum length for a password, from 8 to 32 characters. Default: 8.
	Must Contain	Select the types of characters a password must contain.
	Admin Password Expires after	Select the number of days a password is valid for, after which it must be changed.

Password policy

You can enable and configure password policy for the FortiAnalyzer.

To configure the password policy:

1. Go to *System Settings* > *Admin* > *Admin Settings*.
2. Click to enable *Password Policy*.
3. Configure the following settings, then click *Apply* to apply to password policy.

Minimum Length	Specify the minimum number of characters that a password must be, from 8 to 32. Default: 8.
Must Contain	Specify the types of characters a password must contain: uppercase and lowercase letters, numbers, and/or special characters.
Admin Password Expires after	Specify the number of days a password is valid for. When the time expires, an administrator will be prompted to enter a new password.

Password lockout and retry attempts

By default, the number password retry attempts is set to three, allowing the administrator a maximum of three attempts at logging in to their account before they are locked out for a set amount of time (by default, 60 seconds).

The number of attempts and the default wait time before the administrator can try to enter a password again can be customized. Both settings can be configured using the CLI.

To configure the lockout duration:

1. Enter the following CLI commands:

```
config system global
   set admin-lockout-duration <seconds>
end
```

To configure the number of retry attempts:

1. Enter the following CLI commands:

```
config system global
   set admin-lockout-threshold <failed_attempts>
end
```

Example

To set the lockout threshold to one attempt and set a five minute duration before the administrator can try to log in again, enter the following CLI commands:

```
config system global
   set admin-lockout-duration 300
   set admin-lockout-threshold 1
end
```

GUI language

The GUI supports multiple languages, including:

- English
- Simplified Chinese
- Traditional Chinese
- Japanese
- Korean

By default, the GUI language is set to *Auto Detect*, which automatically uses the language used by the management computer. If that language is not supported, the GUI defaults to English. For best results, you should select the language used by the operating system on the management computer.

For more information about language support, see the FortiAnalyzer Release Notes.

To change the GUI language:

1. Go to *System Settings* > *Admin* > *Admin Settings*.
2. Under the *View Settings*, In the *Language* field, select a language, or *Auto Detect*, from the dropdown list.
3. Click *Apply* to apply the language change.

Idle timeout

To ensure security, the idle timeout period should be short. By default, administrative sessions are disconnected if no activity takes place for five minutes. This idle timeout is recommended to prevent anyone from using the GUI on a PC that was logged in to the GUI and then left unattended. The idle timeout period can be set from 1 to 480 minutes.

To change the idle timeout:

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

Two-factor authentication

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

- FortiAnalyzer
- FortiAuthenticator
- FortiToken

Configuring FortiAuthenticator

On the FortiAuthenticator, you must create a local user and a RADIUS client.

Before proceeding, ensure you have configured your FortiAuthenticator, created a NAS entry for your FortiAnalyzer, and created or imported FortiTokens.

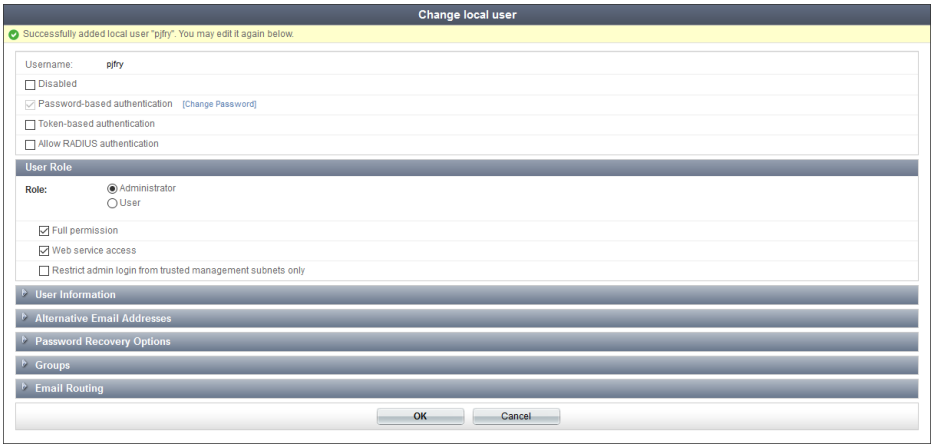
For more information, see the *Two-Factor Authenticator Interoperability Guide* and *FortiAuthenticator Administration Guide* in the Fortinet Document Library.

To create a local user:

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

Username	Enter a user name for the local user.
Password creation	Select Specify a password from the dropdown 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. Click *OK* to continue to the *Change local user* page.



5. Configure the following settings, then click *OK*.

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. Click *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*.

To create a RADIUS client:

1. Go to *Authentication* > *RADIUS Service* > *Clients*.
2. Click *Create New* in the toolbar.
3. Configure the following settings, then click *OK*.

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 Authentication 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 specific user name input formats.
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.

For more information, see the *FortiAuthenticator Administration Guide*, available in the Fortinet Document Library.

Configuring FortiAnalyzer

On the FortiAnalyzer, you need to configure the RADIUS server and create an administrator that uses the RADIUS server for authentication.

To configure the RADIUS server:

1. Go to *System Settings* > *Admin* > *Remote Authentication Server*.
2. Click *Create New* > *RADIUS* in the toolbar.
3. Configure the following settings, then click *OK*.

Name	Enter a name to identify the FortiAuthenticator.
Server Name/IP	Enter the IP address or fully qualified domain name of your FortiAuthenticator.
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.
Port	Enter the port for FortiAuthenticator traffic.
Authentication Type	Select the authentication type the FortiAuthenticator requires. If you select the default *ANY*, FortiAnalyzer tries all authentication types. **Note**: RADIUS server authentication for local administrator users stored in FortiAuthenticator requires the *PAP* authentication type.

To create the administrator:

1. Go to *System Settings* > *Admin* > *Administrator.*
2. Click *Create New* from the toolbar.
3. Configure the settings, selecting the previously added RADIUS server from the *RADIUS Server* dropdown list. See Creating administrators on page 55.
4. Click *OK* to save the settings.

To test the configuration:

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

Device Manager

Use the *Device Manager* pane to add, configure, and manage devices and VDOMs.

If FortiManager features are enabled, then this is the FortiManager Device Manager.

For information about using FortiManager features, see the *FortiManager Administration Guide* or the FortiManager Online Help.

After you add and register a device or VDOM, the FortiAnalyzer unit starts collecting logs from that device or VDOM. You can configure the FortiAnalyzer unit to forward logs to another device. See Log Forwarding on page 191.

ADOMs

You can organize connected devices into ADOMs to better manage the devices. ADOMs can be organized by:

- Firmware version: group all 5.4 devices into one ADOM, and all 5.2 devices into another.
- Geographic regions: group all devices for a specific geographic region into an ADOM, and devices for a separate region into another ADOM.
- Administrator users: group devices into separate ADOMs based for specific administrators responsible for the group of devices.
- Customers: group all devices for one customer into an ADOM, and devices for another customer into another ADOM.

  FortiAnalyzer, FortiCache, FortiClient, FortiDDos, FortiMail, FortiManager, FortiSandbox, FortiWeb, Chassis, and FortiCarrier devices are automatically placed in their own ADOMs.

Each administrator profile can be customized to provide read-only, read/write, or restrict access to various ADOM settings. When creating new administrator accounts, you can restrict which ADOMs the administrator can access, for enhanced control of your administrator users. For more information on ADOM configuration and settings, see Administrative Domains on page 43.

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 the right-click menu.

Using FortiManager to manage FortiAnalyzer devices

You can add FortiAnalyzer devices to FortiManager and manage them. When you add a FortiAnalyzer device to FortiManager, FortiManager automatically enables FortiAnalyzer features. FortiAnalyzer and FortiManager must be running the same OS version, at least 5.6 or later.

In the *Device Manager* pane, a message informs you the device is managed by FortiManager and all changes should be performed on FortiManager to avoid conflict. The top right of this pane displays a lock icon. If ADOMs are enabled, the *System Settings > All ADOMs* pane displays a lock icon beside the ADOM managed by FortiManager.

Logs are stored on the FortiAnalyzer device, not the FortiManager device. You configure log storage settings on the FortiAnalyzer device; you cannot change log storage settings using FortiManager.

For more information, see Adding FortiAnalyzer devices in the the *FortiManager Administration Guide* or the FortiManager Online Help.

Adding devices

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

You must configure devices to send logs to FortiAnalyzer. For example, after you add and register a FortiGate device with FortiAnalyzer, you must also configure the FortiGate device to send logs to FortiAnalyzer. In the FortiGate GUI, go to *Log & Report > Log Settings*, and enable *Send Logs to FortiAnalyzer/FortiManager*.

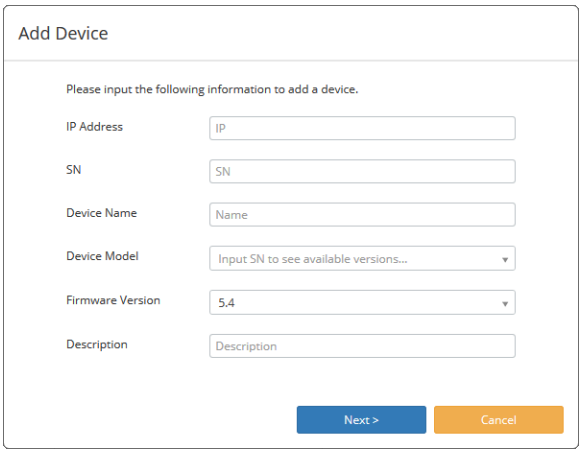
If you are using high availability, you must specify the FortiGate HA group name when adding a FortiGate cluster.

Adding devices using the wizard

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

To add devices using the wizard:

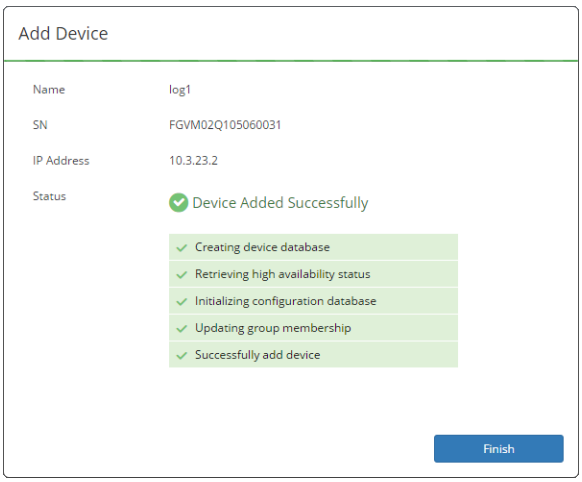
1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Device Manager* and click *Add Device*.



3. Configure the following settings:

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).

4. Click *Next*.
   The device is added to the ADOM and, if successful, is ready to begin sending logs to the FortiAnalyzer unit.



5. Click *Finish* to finish adding the device and close the wizard.

Adding devices manually

You can configure supported devices to send logs to the FortiAnalyzer device. These devices are 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 can start receiving logs from the device.

When ADOMs are enabled, you can assign the device to an ADOM. When manually adding multiple devices at one time, they are all added to the same ADOM.

When you delete a device or VDOM from the FortiAnalyzer unit, its raw log files are also deleted. SQL database logs are not deleted.

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.

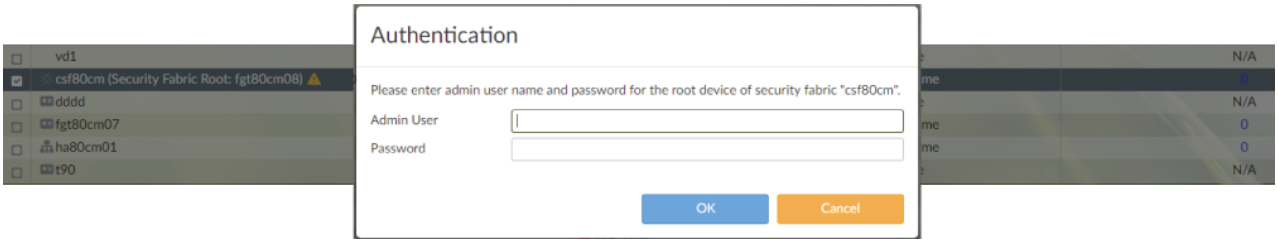
Adding a security fabric group

Before you can add a security fabric group to FortiAnalyzer, you need to create the security fabric group in FortiGate. For more information, see the *FortiOS Handbook*.

Fortinet recommends using a dedicated Super_User administrator account on the FortiGate for FortiAnalyzer access. This ensures that associated log messages are identified as originating from FortiAnalyzer activity. This dedicated Super_User administrator account only needs *Read Only* access to *System Configuration*; all other access can be set to *None*.

To add a security fabric group:

1. Go to *Device Manager* > *Unregistered Devices*.
2. Select all the devices corresponding to the security fabric group created in FortiGate.
3. Authenticate the security fabric group by clicking the *Warning* icon (yellow triangle) beside the corresponding FortiGate root.



4. Enter the *Authentication Credentials*. The authentication credentials are the ones you specified in FortiGate. Once the FortiGate root has been authenticated, the *Warning* icon will disappear.

5. After authentication, it takes a few minutes for FortiAnalyzer to automatically populate the devices under the FortiGate root which creates the security fabric group.

Managing devices

Use the tools and commands in the *Device Manager* pane to manage devices and VDOMs.

Using 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.

The *Devices Total*, *Devices Unregistered*, and the *Devices Log Status Down* tabs include the following default columns:

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. A lock icon displays when a secure tunnel is being used to transfer logs from the device to the FortiAnalyzer unit.
Average Log Rate (Logs/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.
Device Storage	Displays how much of the allotted disk space has been consumed by logs.
Description	Displays a description of the device (not displayed in *Devices Unregistered* tab).

Using the toolbar

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

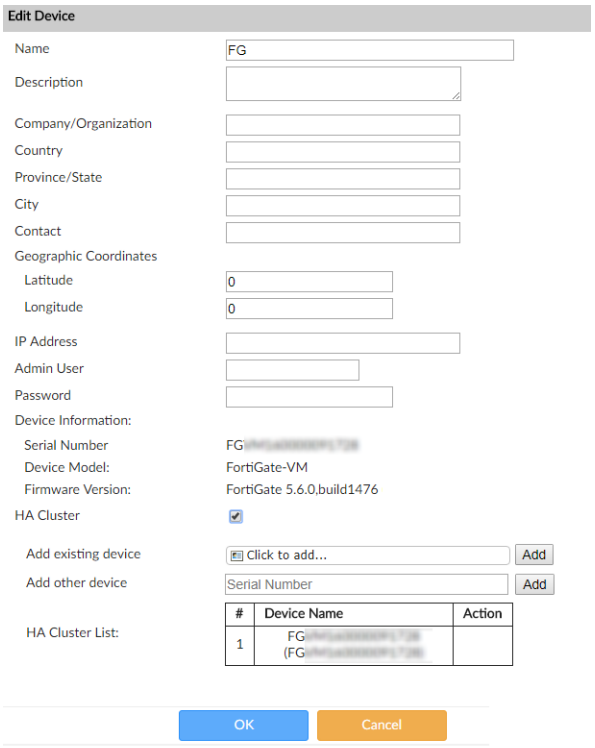
Button	Description
Add Device	Opens the *Add Device Wizard* to add a device to the FortiAnalyzer unit. The device is added, but not registered with the FortiAnalyzer unit. Unregistered devices are displayed in the *Unregistered Devices* tree menu.
Edit	Edits the selected device.
Delete	Deletes the selected devices or VDOMs from the FortiAnalyzer unit. When you delete a device, its raw log files are also deleted. SQL database logs are not deleted.
Column Settings	Click to select which columns to display or select *Reset to Default* to display the default columns.
More	Displays more menu items including *Import Device List* and *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.

Editing device information

Use the *Edit Device* page to edit information about a device. The information and options available on the *Edit Device* page depend on the device type, firmware version, and which features are enabled.

To edit information for a device or model device:

1. Go to *Device Manager* and click the *Devices Total* tab in the quick status bar.
2. In the content pane, select the device or model device, and click *Edit*. The *Edit Device* pane displays.



3. Edit the device settings as required.

Name	The name of the device.
Description	Descriptive information about the device.
Company/Organization	Company or organization information.
Country	Type the country.
Province/State	Type the province or state.
City	Type the city.
Contact	Type the contact information.
Geographic Coordinates	Identifies the latitude and longitude of the device location to support the interactive maps.
IP Address	The IP address of the device.
Pre-Shared Key	The model device's pre-shared key. Select *Show Pre-shared Key* to see the key. This option is only available when editing a model device that was added with a pre-shared key.
Admin User	The administrator user name.
Password	The administrator user password.
Device Information	Information about the device, including some or all of: serial number, device model, firmware version, connected interface, HA mode, cluster name, and cluster members.
HA Cluster	Select to identify the device as part of an HA cluster, and to identify the other device in the cluster.

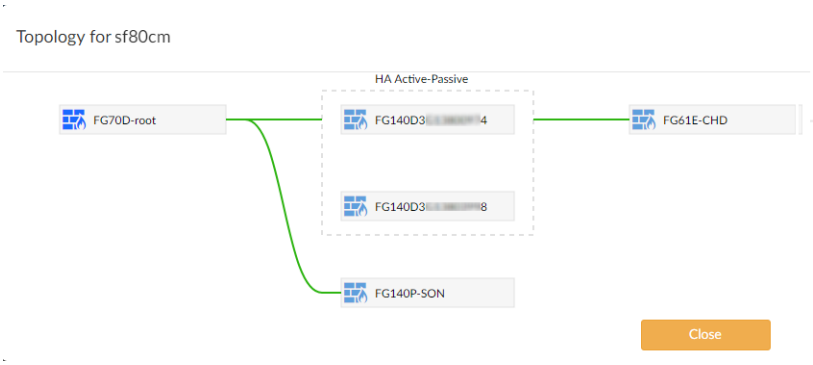
4. After making the appropriate changes click *OK*.

Displaying security fabric topology

For security fabric devices, you can display the security fabric topology.

To display the security fabric topology:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Device Manager* and click the *Devices Total* tab in the quick status bar.
3. Right-click a security fabric device and select *Fabric Topology*.
   A pop-up window displays the security fabric topology for that device.
   If you selected *Fabric Topology* by right-clicking a device within the security fabric group, the device is highlighted in the topology. If you selected *Fabric Topology* by right-clicking the name of the security fabric group, no device is highlighted in the topology.

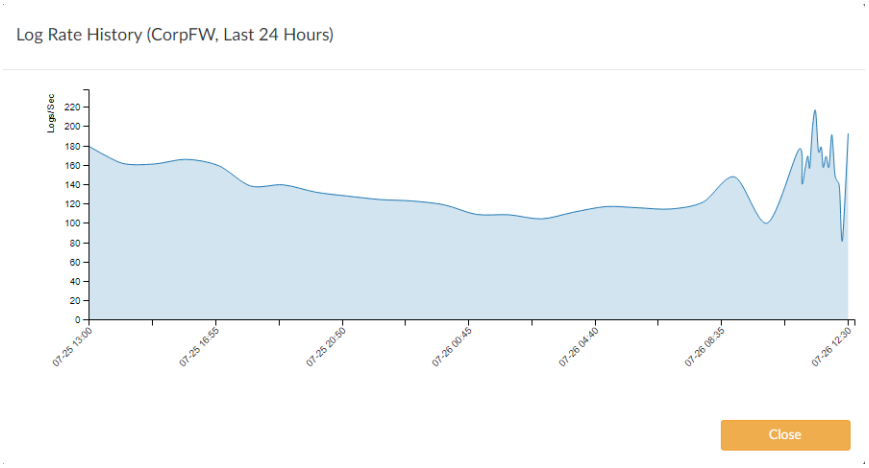


Displaying historical average log rates

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

To display historical average logs rates:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Device Manager* and click the *Devices Total* tab in the quick status bar.
3. In the *Average Log Rate (Logs/Sec)* column, click the number to display the graph.



4. Hover the cursor over the graph to display more details.

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. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *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.

Log and file storage

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

When ADOMs are enabled, settings can be specified for each ADOM that apply only to the devices in it. When ADOMs are disabled, the settings apply to all managed devices.

Data policy and disk utilization settings for devices are collectively called log storage settings. Global log and file storage settings apply to all logs and files, regardless of log storage settings (see File Management on page 221). Both the global and log storage settings are always active.

Disk space allocation

On the FortiAnalyzer, the system reserves 5% to 20% of the disk space for system usage and unexpected quota overflow. The remaining 80% to 95% of the disk space is available for allocation to devices.

Reports are stored in the reserved space.

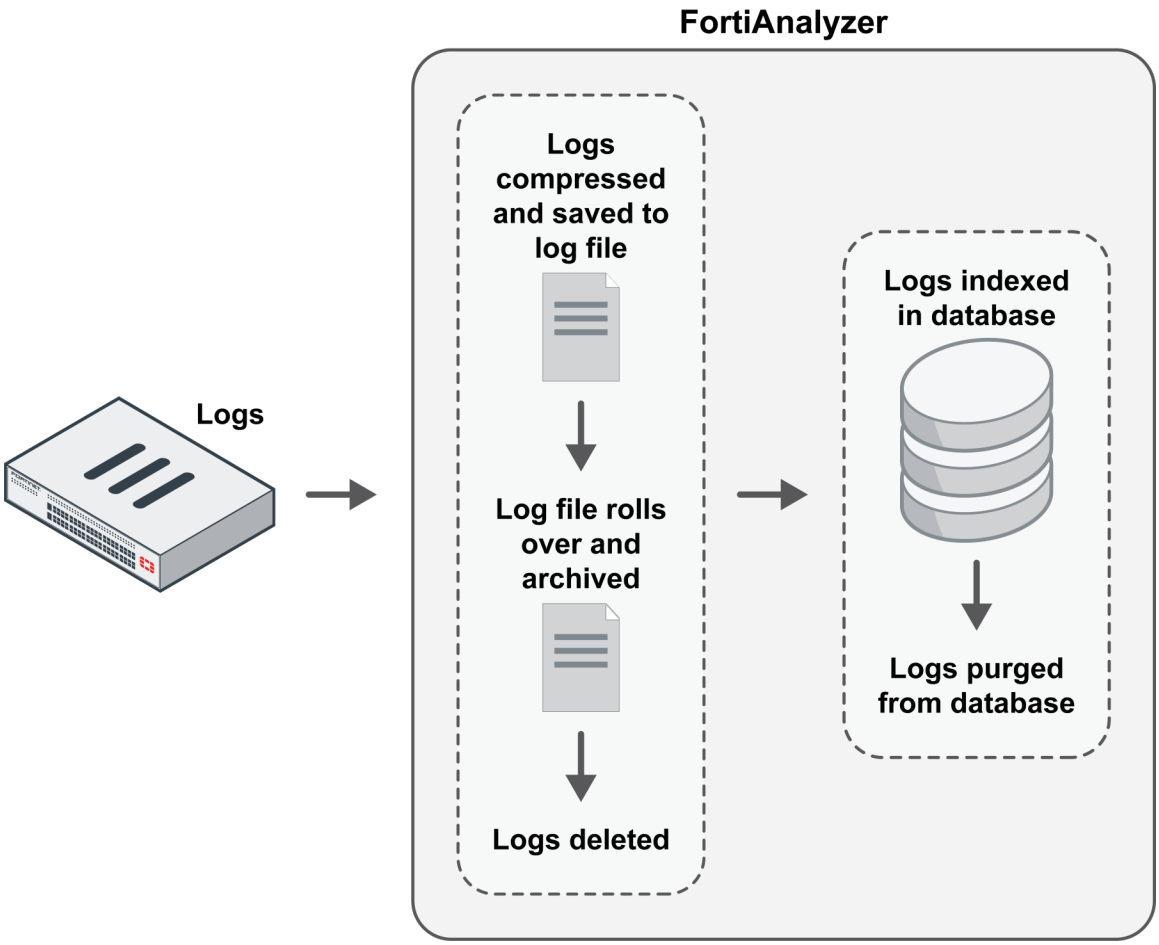
Total Available Disk Size	Reserved Disk Quota
Small Disk (up to 500GB)	The system reserves either 20% or 50GB of disk space, whichever is smaller.
Medium Disk (up to 1TB)	The system reserves either 15% or 100GB of disk space, whichever is smaller.
Large Disk (up to 3TB)	The system reserves either 10% or 200GB of disk space, whichever is smaller.
Very Large Disk (up to 5TB)	The system reserves either 5% or 300GB of disk space, whichever is smaller.

The RAID level you select determines the disk size and the reserved disk quota level. For example, a FortiAnalyzer 1000C with four 1TB disks configured in RAID 10 is considered a very large disk, so 5%, or 300GB of disk space is reserved.

Log and file workflow

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

1. Logs are compressed and saved in a log file on the FortiAnalyzer disks.
   When a log file reaches a specified size, FortiAnalyzer rolls it over and archives it, and creates a new log file to receive incoming logs. You can specify the size at which the log file rolls over. See Device logs on page 217.
2. Logs are indexed in the SQL database to support analysis.
   You can specify how long to keep logs indexed using a data policy. See Log storage policy on page 89.
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 using a data policy. See Log storage policy on page 89.



In the indexed phase, logs are indexed in the SQL database for a specified length of time so they can be used for analysis. Indexed, or Analytics, logs are considered online, and details about them can be used viewed in the *FortiView*, *NOC*, *Log View*, and *Event Management* modules. You can also generate reports about the logs in the *Reports* pane.

In the compressed phase, logs are compressed and archived in FortiAnalyzer disks for a specified length of time for the purpose of retention. Compressed, or Archived, logs are considered offline, and their details cannot be immediately viewed or used to generate reports.

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

Log Phase	Location	Immediate Analytic Support
Indexed	Compressed in log file and indexed in SQL database	Yes. Logs are available for analytic use in *FortiView*, *NOC*, *Event Management*, and *Reports*.
Compressed	Compressed in log file	No.

Automatic deletion

Logs and files are automatically deleted from the FortiAnalyzer unit according to the following settings:

- Global automatic file deletion

  File management settings specify when to delete the oldest Archive logs, quarantined files, reports, and archived files from the disks, regardless of the log storage settings. See File Management on page 221 for information.
- Data policy

  Data policies specify how long to store Analytics and Archive logs for each device. When the specified length of time expires, Archive logs for the device are automatically deleted from the FortiAnalyzer device's disks.
- Disk utilization

  Disk utilization settings delete the oldest Archive logs for each device when the allotted disk space is filled. The allotted disk space is defined by the log storage settings. Alerts warn you when the disk space usage reaches a configured percentage.

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 are automatically deleted regardless of the log storage settings associated with the device.

The following table summarizes the automatic deletion polices:

Policy	Scope	Trigger
Global automatic file deletion	All logs, files, and reports on the system	When the specified length of time expires, old files are automatically deleted. This policy applies to 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 length 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.
Disk utilization	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.

Logs for deleted devices

When you delete one or more devices from FortiAnalyzer, the raw log files and archive packets are deleted, and the action is recorded in the local event log. However, the logs that have been inserted into the SQL database are not deleted from the SQL database. As a result, logs for the deleted devices might display in the *Log View* and *FortiView* panes, and any reports based on the logs might include results.

The following are ways you can remove logs from the SQL database for deleted devices.

- Rebuild the SQL database for the ADOM to which deleted devices belonged or rebuild the entire SQL database.
- Configure the log storage policy. When the deleted device logs are older than the *Keep Logs for Analytics* setting, they are deleted. Also, when analytic logs exceed their disk quota, the SQL database is trimmed starting with the oldest database tables. For more information, see Configure log storage on page 90.

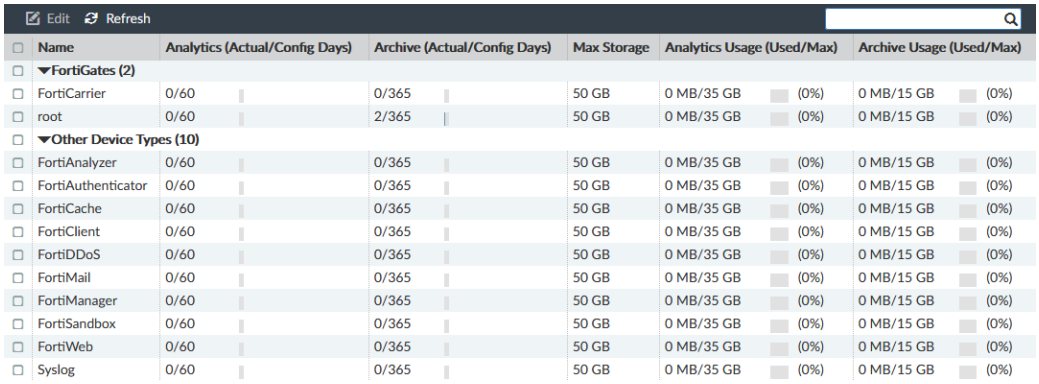
- Configure global automatic file deletion settings in *System Settings* > *Advanced* > *File Management*. When the deleted device logs are older than the configured setting, they are deleted. For more information, see File Management on page 221.

File Management configures global settings that override other log storage settings and apply to all ADOMs.

Log storage policy

The log storage policy affects only the logs and SQL database of the devices associated with the log storage policy. Reports are not affected. See Disk space allocation on page 86.

If ADOMs are enabled, you can view the data policies and disk usage for each ADOM in *System Settings* > *Storage Info*.



Edit Refresh

Name	Analytics (Actual/Config Days)	Archive (Actual/Config Days)	Max Storage	Analytics Usage (Used/Max)	Archive Usage (Used/Max)
FortiGates (2)					
FortiCarrier	0/60	0/365	50 GB	0 MB/35 GB (0%)	0 MB/15 GB (0%)
root	0/60	2/365	50 GB	0 MB/35 GB (0%)	0 MB/15 GB (0%)
Other Device Types (10)					
FortiAnalyzer	0/60	0/365	50 GB	0 MB/35 GB (0%)	0 MB/15 GB (0%)
FortiAuthenticator	0/60	0/365	50 GB	0 MB/35 GB (0%)	0 MB/15 GB (0%)
FortiCache	0/60	0/365	50 GB	0 MB/35 GB (0%)	0 MB/15 GB (0%)
FortiClient	0/60	0/365	50 GB	0 MB/35 GB (0%)	0 MB/15 GB (0%)
FortiDDoS	0/60	0/365	50 GB	0 MB/35 GB (0%)	0 MB/15 GB (0%)
FortiMail	0/60	0/365	50 GB	0 MB/35 GB (0%)	0 MB/15 GB (0%)
FortiManager	0/60	0/365	50 GB	0 MB/35 GB (0%)	0 MB/15 GB (0%)
FortiSandbox	0/60	0/365	50 GB	0 MB/35 GB (0%)	0 MB/15 GB (0%)
FortiWeb	0/60	0/365	50 GB	0 MB/35 GB (0%)	0 MB/15 GB (0%)
Syslog	0/60	0/365	50 GB	0 MB/35 GB (0%)	0 MB/15 GB (0%)

The following information and options are available:

Edit	Edit the selected ADOM's log storage policy.
Refresh	Refresh the page.
Search	Enter a search term to search the list.
Name	The name of the ADOM. ADOMs are listed in two groups: *FortiGates* and *Other Device Types*.
Analytics (Actual/Config Days)	The age, in days, of the oldest Analytics logs (Actual Days), and the number of days Analytics logs will be kept according to the data policy (Config Days).
Archive (Actual/Config Days)	The age, in days, of the oldest Archive logs (Actual Days) and the number of days Archive logs will be kept according to the data policy (Config Days).
Max Storage	The maximum disk space allotted to the ADOM (for both Analytics and Archive logs). See Disk space allocation on page 86 for more information.

Analytics Usage (Used/Max)	How much disk space Analytics logs have used, and the maximum disk space allotted for them.
Archive Usage (Used/Max)	How much disk space Archive logs have used and the maximum disk space allotted for them.

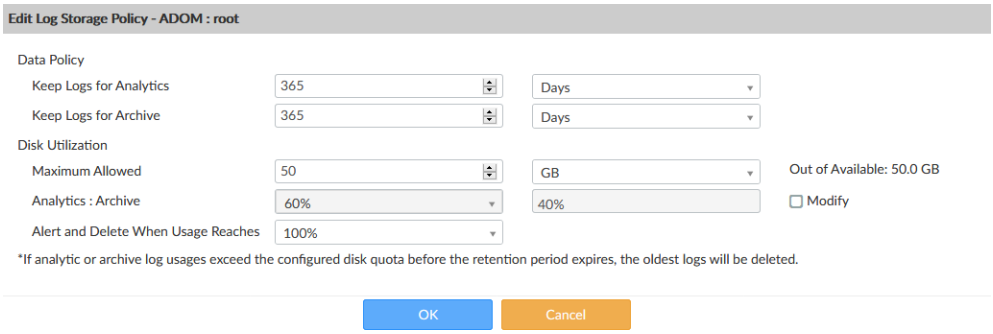
Configure log storage

The log storage policy affects the logs and SQL database of the device associated with the log storage policy.

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

To configure log storage settings:

1. Go to *System Settings* > *Storage Info*.
2. Double-click on an ADOM, right-click on an ADOM and then select *Edit* from the menu, or select the ADOM then click *Edit* in the toolbar. The *Edit Log Storage Policy* pane opens.



3. Configure the following settings, then click *OK*.

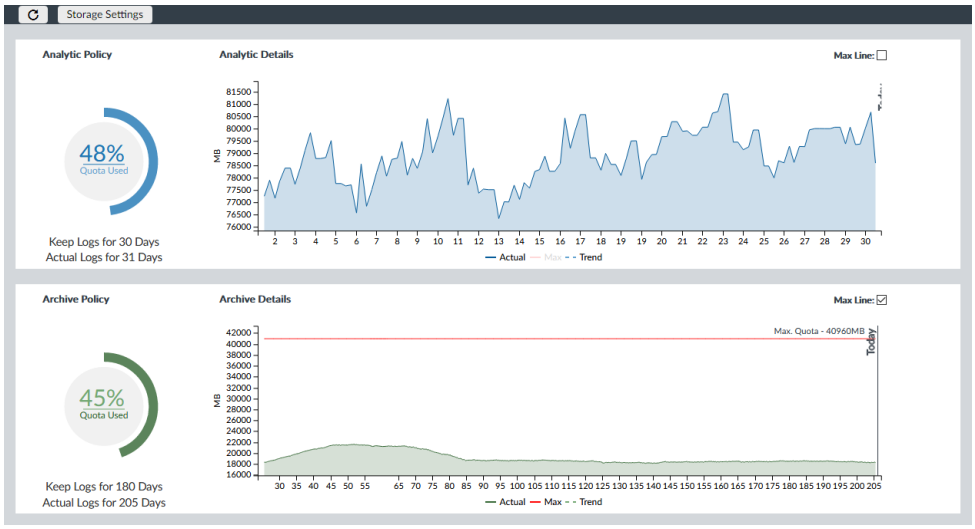
Data Policy		
	Keep Logs for Analytics	Specify how long to keep Analytics logs.
	Keep Logs for Archive	Specify how long to keep Archive logs. Make sure your setting meets your organization's regulatory requirements.
Disk Utilization		
	Maximum Allowed	Specify the amount of disk space allotted. See also Disk space allocation on page 86.
	Analytics : Archive	Specify the disk space ratio between Analytics and Archive logs. Analytics logs require more space than Archive logs. Click the *Modify* checkbox to change the setting.

Alert and Delete When Usage Reaches	Specify the percentage of allotted disk space usage that will trigger an alert messages and start automatically deleting logs. The oldest Archive log files or Analytics database tables are deleted first.

Storage statistics

To open the *Storage Statistics* pane, go to *Log View* > *Storage Statistics*, or in the *Device Manager* quick status bar, click *Storage Used*.

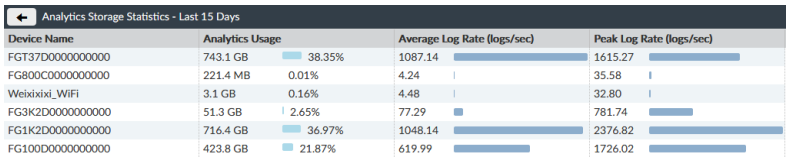
The pane shows visualizations of disk space usage for Analytic and Archive logs. The policy diagrams show an overview and the details graphs show disk space usage details.



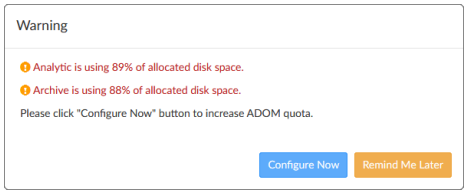
The policy diagram shows the percentage of the disk space quota that is used. Hover your cursor over the diagram to view the used, free, and total allotted disk space. The configured length of time that logs are stored is also shown.

To view or change log storage policies, click *Storage Settings* in the toolbar to open the *Edit Log Storage Policy* dialog box.

The details graph shows the amount disk space used, in MBs, over the time period that the logs are stored for. Click *Max Line* to show a line on the graph for the total space allotted. Hover over a spot in the graph to view the used and available disk space at that specific date and time. Click on a point in the details graph to open a breakdown of the disk space usage by device.



When the used quota approaches 100 percent, a warning message displays when accessing the *Storage Statistics* pane.



Click *Configure Now* to open the *Edit Log Storage Policy* dialog box where you can adjust log storage policies to prevent running out of allocated space (see Configure log storage on page 90), or click *Remind Me Later* to resolve the issue another time.

FortiView

FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

FortiView allows you to use multiple filters in the consoles, enabling you to narrow your view to a specific time, by user ID or local IP address, by application, and others. You can use it to investigate traffic activity such as user uploads/downloads or videos watched on YouTube on a network-wide user group or on an individual-user level. It presents information in both text and visual format.

You can view summaries of log data in *FortiView* such as top threats to your network, top sources of network traffic, and top destinations of network traffic. Depending on which summary you are viewing, you can view summary information in different formats: table, bubble, map, or tile. For each summary view, you can drill down to see more details.

FortiGate, FortiCarrier, and FortiClient EMS devices support FortiView.

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. You can select which widgets to display in the *Summary*.

Category	View	Description
Threats	Top Threats	Lists the top threats to your network. The following incidents are considered threats: • Risk applications detected by application control. • Intrusion incidents detected by IPS. • Malicious web sites detected by web filtering. • Malware/botnets detected by antivirus. **Note**: If FortiGate is running FortiOS 5.0.x, turn on *Security Profiles* > *Client Reputation* 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. The list of threats at the bottom shows the location, threat, severity, and time of the attacks. The color gradient of the darts on the map indicate the traffic risk, where red indicates the more critical risk. This view has no filtering options. See also Viewing the threat map on page 101.
	Indicators of Compromise (IOC)	Displays end users with suspicious web use compromises, including end users' IP addresses, overall threat rating, and number of threats. **Note**: To use this feature: 1. UTM logs of the connected FortiGate devices must be enabled. 2. The FortiAnalyzer must subscribe to FortiGuard to keep its threat database current.
Traffic	Top Sources	Displays the highest network traffic by source IP address and interface, device, threat score (blocked and allowed), sessions (blocked and allowed), and bytes (sent and received).
	Top Destinations	Displays the highest network traffic by destination IP addresses, the applications used to access the destination, sessions, and bytes.
	Top Countries	Displays the highest network traffic by country in terms of traffic sessions, including the destination, threat score, sessions, and bytes.
	Policy Hits	Lists the policy hits by policy, device name, VDOM, number of hits, bytes, and last used time and date.

Category	View	Description
Applications & Websites	Top Applications	Displays the top applications used on the network including the application name, category, risk level, number of clients, sessions blocked and allowed, and bytes sent and received. For a usage example, see Finding application and user information on page 104.
	Top Cloud Applications	Displays the top cloud applications used on the network.
	Top Websites	Displays the top allowed and blocked web sites on the network. You can view information by domain or category by using the options in the top right of the toolbar.
	Top Browsing Users	Displays the top web-browsing users, including source, group, 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.
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.

Category	View	Description
Endpoints	All Endpoints	Lists the FortiClient endpoints registered to the FortiGate device.
	Top Vulnerabilities	Displays vulnerability information about the FortiClient endpoints registered to specific FortiGate devices. View by *Device* or *Vulnerability*. In *Device* view, the table shows the device, source, number and severity of vulnerabilities, and category. In *Vulnerability* view, select table or bubble format. The table format shows the vulnerability name, severity, category, CVE ID, and host count. The bubble graph format shows vulnerability by severity and frequency.
	Top Threats	Displays the top threats for registered FortiClient endpoints, including the threat, threat level, and the number of incidents (blocked and allowed).
	Top Applications	Displays the top applications used by registered FortiClient endpoints, including the application name, risk level, sessions blocked and allowed, and bytes sent and received.
	Top Web Sites	Displays the top allowed and blocked web sites on the network.

FortiView summaries for FortiClient EMS devices

Category	View	Description
Threats	Top Threats	Lists the top users involved in incidents and the top threats to your network. The following incidents are considered threats: • Risk applications detected by application control • Malicious web sites detected by web filtering • Malware/botnets detected by antivirus
Applications & Websites	Top Applications	Displays the top applications used on the network including the application name, category, risk level, number of clients, sessions blocked and allowed, and bytes sent and received.
	Top Websites	Displays the top allowed and blocked web sites on the network.
Endpoints	All Endpoints	Lists the FortiClient endpoints registered to the FortiClient EMS device.
	Top Vulnerabilities	Displays vulnerability information about the FortiClient endpoints that are registered to the FortiClient EMS device. View by *Device* or *Vulnerability*. In *Device* view, the table shows the device, source, number and severity of vulnerabilities, and category. In *Vulnerability* view, select table or bubble format. The table format shows the vulnerability name, severity, category, CVE ID, and host count. The bubble graph format shows vulnerability by severity and frequency.

Using FortiView

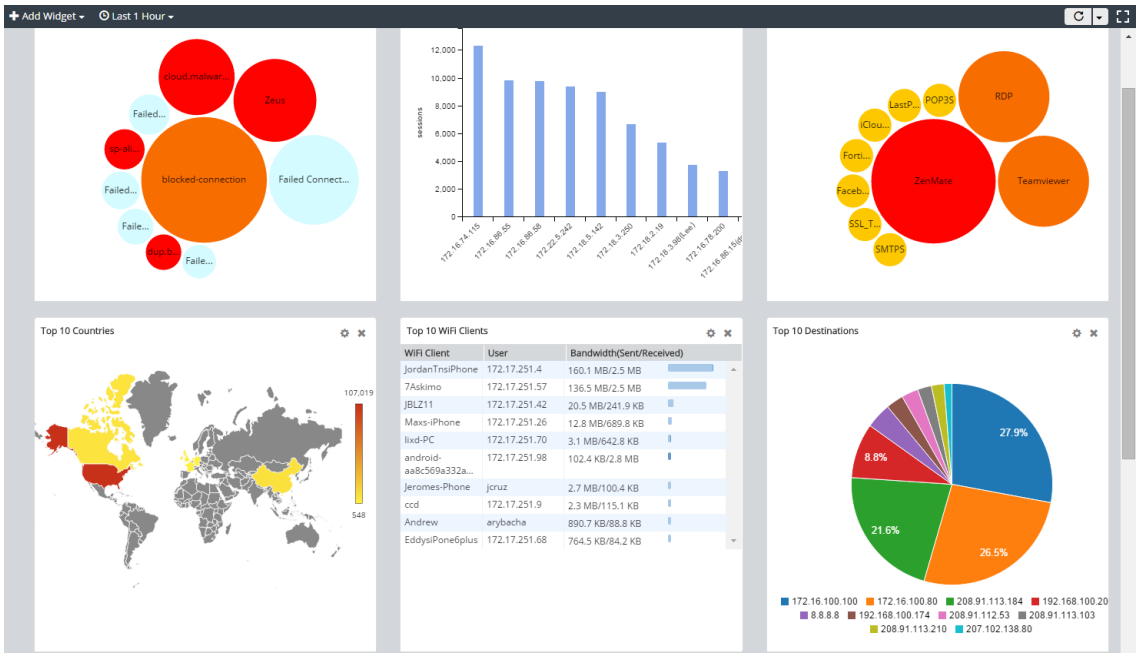
When ADOMs are enabled, *FortiView* displays information for each ADOM so ensure you are in the correct ADOM. See Switching between ADOMs on page 25.

FortiView Summary

The *FortiView Summary* shows you an overview of the most used summary views. You can configure the overall view of the *Summary*.

Each summary view is a widget. You can configure the view settings of each widget, including adding the same widget multiple times, each showing a different view. For example, you can add two Top Threats widgets: one showing the Top 10 Threats view in a bubble chart, and the other showing the Top 20 Threats in a table.

To view the details of each summary view, you can drill down each summary view or use the tree menu to see an individual view.

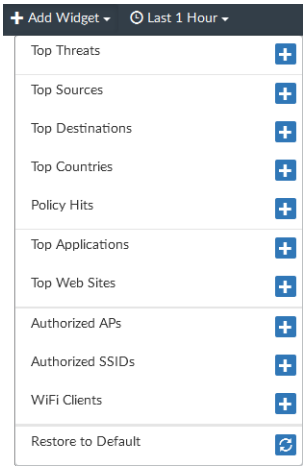


Configuring the overall view settings of the Summary

To add a widget to the Summary:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *FortiView*.

3. In the content pane toolbar, click *Add Widget* and select a FortiView summary from the list.



To remove a widget from the Summary:

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

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

On the *FortiView Summary*, select a time period from the *time period* dropdown list in the toolbar.

To refresh the view and/or set refresh rate:

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

To switch to full-screen mode:

On the *FortiView Summary*, click the *Full Screen* button in the toolbar. To exit full-screen mode, either press *Esc* or click the *Exit Full Screen* button in the top-right.

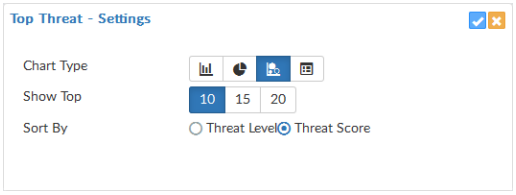
Viewing each widget on the Summary

You can view and drill down each summary view on the *Summary* or you can view an individual page that you access through the tree menu. See Filtering FortiView summaries on page 102.

Configuring the view settings for an individual widget

To Configure the view settings of an individual widget:

1. On the *FortiView Summary*, click the *Edit Settings* button in the top-right 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* in the top-right corner to save the changes.

Viewing FortiView summaries

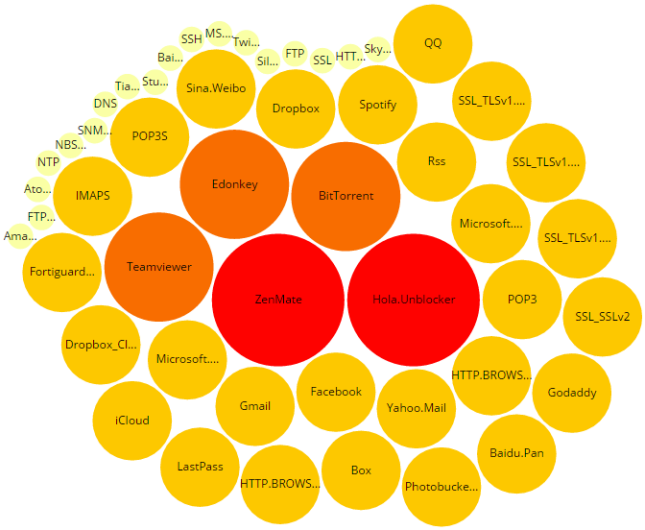
When viewing summaries, use the controls in the toolbar to select a display format, select a device, specify a time period, refresh the view, set the refresh rate, export the information, and switch to full-screen mode.

Depending on which summary you are viewing, you can view summary information in different formats such as table, bubble, map, or tile.

Some summary views support only one format. For example, *Threat Map* only supports the map format and *Policy Hits* supports only the table format.

- In summary views that support multiple formats, click the format icon in the top-right to select another format.
- In simple format:
  - To select which items to display, use the *Sort By* dropdown list in the top-left.
- In table format:
  - To select how many items to display, use the *Show* dropdown list in the bottom-right.
  - To sort by a column, click the column title.

- In bubble and map format:
  - If sorting is available, use the *Sort By* dropdown list in the top-right.
  - To view more information, hover the mouse over a graphical element.



Most summary views let you drill down to view more details. To drill down to view more details, click or right-click an element to view details about different dimensions in different tabs. You can continue to drill down by double-clicking an entry. Click the *Back* button in the toolbar to return to the previous view.

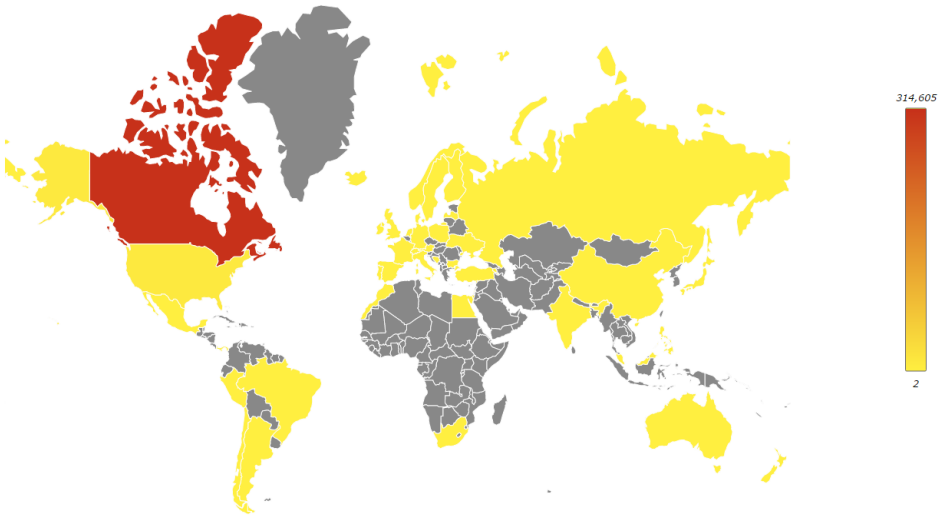
Some summary views support multiple views. For example, *Endpoints* > *Top Vulnerabilities* has a *Device* view and a *Vulnerability* view; and *Applications & Websites* > *Top Cloud Applications* has a *Cloud Application* view and a *Cloud User* view.

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 dropdown list in the top-right.



3. Choose a sort method from the *Sort By* list in the top-right.
4. To view more information, hover the mouse over the map.
5. To drill down to view more details, click a country to view details about different dimensions in different tabs.
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 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

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

To filter FortiView summaries using filters in the toolbar:

1. Specify filters in the *Add Filter* box.
   - Regular Search: In the selected summary view, click *Add Filter* and select a filter from the dropdown list, then type a value. Click NOT to negate the filter value. You can add multiple filters and connect them with “and” or “or”.
   - Advanced Search: Click the *Switch to Advanced Search* icon at the right end of the *Add Filter* box. In Advanced Search mode, enter the search criteria (log field names and values). Click the *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. If necessary, click *Go*.

To filter FortiView summaries using the right-click menu:

In the selected summary view, right-click an entry and select a filter criterion (*Search <filter value>*).

Depending on the column in which your mouse is placed when you right-click, *FortiView* uses the column value 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 related logs, the same filters that you 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

You can export filtered *FortiView* summaries or any level of the drilldowns to PDF and report charts. Filtered summaries are always exported in table format.

To export a filtered summary:

1. In the filtered summary view or its drilldown, click the *Export* button in the top-right and select *Export to PDF* or *Export to Report Chart*.
2. In the dialog box, review and configure settings:
   - Specify a file name for the exported file.
   - In the *Top* field, specify the number of entries to export.
   - If you are in a drilldown view, the tab you are in is selected by default. You can select more tabs. If you are exporting to report charst, the export creates one chart for each tab.
3. Click *OK*.

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

Only log field filters are exported. Device and time period filters are not exported.

FortiView Indicators of Compromise

The *Indicators of Compromise* (IOC) summary shows end users with suspicious web usage compromises. It provides information such as end users' IP addresses, last detected date, host name, OS, a *Map View*, and number of threats. You can drill down to view threat details.

FortiAnalyzer generates the *Indicators of Compromise* by checking 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 complete, FortiAnalyzer aggregates all the threat scores of an end user and gives its verdict of the end user's overall Indicators of Compromise.

To use this Indicators of Compromise 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 synchronized with the FortiGuard threat database. See Subscribing FortiAnalyzer to FortiGuard on page 103.

Viewing Indicators of Compromise information

Indicators of Compromise information is in *FortiView* > *Threats* > *Indicators of Compromise*.

When viewing Indicators of Compromise, use the controls in the toolbar to select *Table* or *Tile* format, select devices, specify a time period, refresh the view, set the refresh rate, export the information, and switch to full-screen mode.

In tile format, you can view a map of the Indicators of Compromise by clicking *Map View* in the tile. To see more details, hover the cursor over a destination

To acknowledge the Indicators of Compromise of an end user, click *Ack*.

To filter entries, click *Add Filter* and specify devices or a time period.

To drill down and view threat details, double-click a tile or a row.

Subscribing FortiAnalyzer to FortiGuard

Your FortiAnalyzer needs to subscribe to FortiGuard to keep its threat database up to date. You must purchase a FortiGuard Indicators of Compromise Service license for that.

To subscribe FortiAnalyzer to FortiGuard:

1. Go to *System Settings* > *Dashboard*.
2. In the *License Information* widget, find the *FortiGuard* > *Indicators of Compromise 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) 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.

Go to *FortiView* > *System* > *Resource Usage* to monitor resource usage for devices.

Examples of using FortiView

You can use FortiView to find information about your network. The following are some examples.

Finding application and user information

Company ABC has over 1000 employees using different 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 application and user information:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *FortiView* > *Applications & Websites* > *Top Applications*.
3. Click *Add Filter*, 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 IP*, 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 the sales team uses.

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

The network administrator already monitors unknown applications using FortiAnalyzer alerts and was informed an unauthorized program had been installed. Following an investigation, the administrator determined 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. If using ADOMs, ensure you are in the correct ADOM.
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 analyze and report on the top source and destinations students visit, 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. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *FortiView* > *Traffic* > *Top Sources*.
3. Go to *FortiView* > *Traffic* > *Top Destinations*.

Viewing vulnerabilities with high severity and frequency

A-One Company experiences many network vulnerabilities but most of them are of low to medium severity and occur infrequently. The network administrator wants to quickly see which vulnerabilities have high severity and frequency.

To view vulnerabilities with high severity and frequency:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *FortiView* > *Endpoints* > *Top Vulnerabilities*.
3. In the toolbar, select *Vulnerability* and *Bubble* format.

Focus on the top right of the bubble chart which shows vulnerabilities with the highest severity and frequency. Hover the cursor over a vulnerability to see additional information and click a vulnerability to drill down to view more details.

NOC

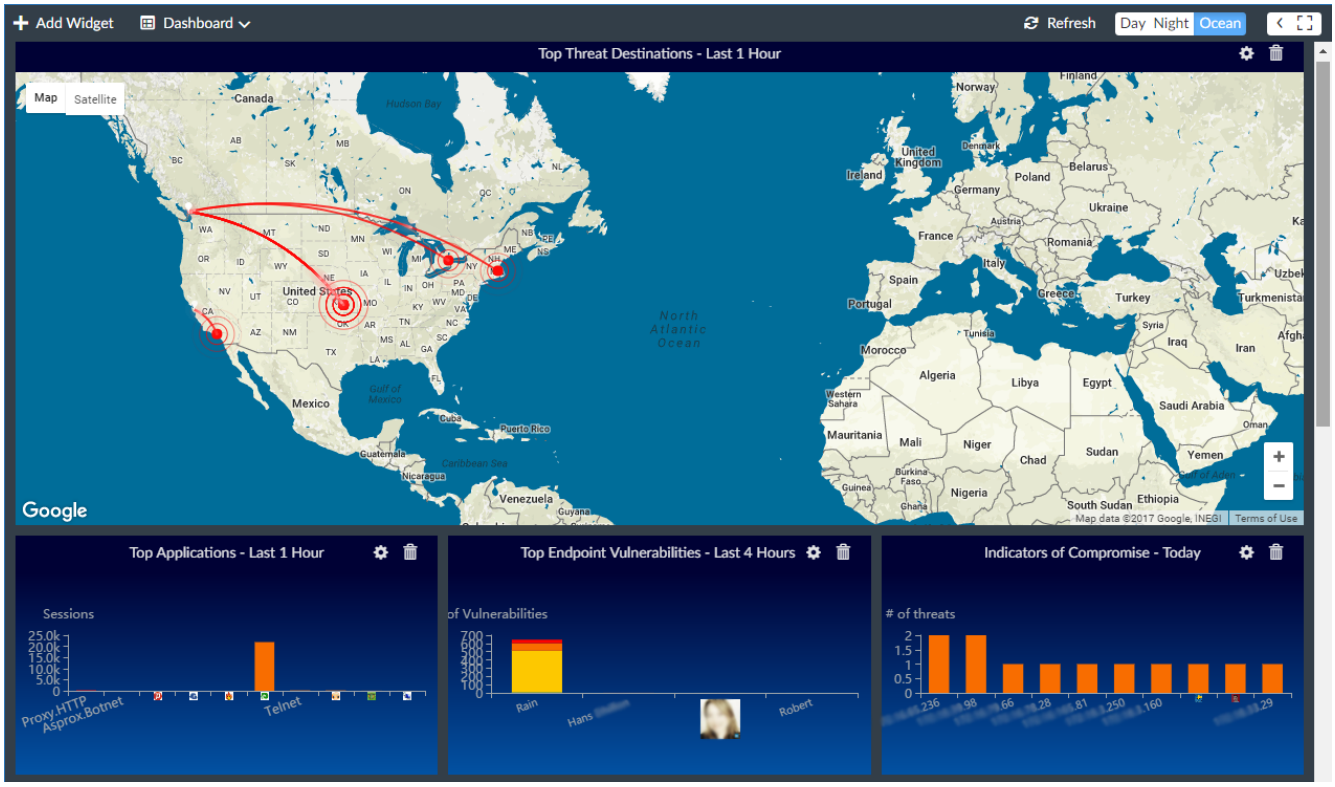
Use the NOC (Network Operations Center) or SOC (Security Operations Center) to view multiple panes of network activity, including monitoring network security, WiFi security, and system performance.

NOC displays both real-time monitoring and historical trends. This centralized monitoring and awareness help you to effectively monitor network events, threats, and security alerts.

NOC Dashboard

NOC includes predefined Security Monitor, WiFi Monitor, and System Performance dashboards.

You can create custom dashboards and add widgets to them. Each pane or widget monitors one activity. You can select what widgets to display, customize widgets, move and resize widgets, and display widgets in full screen or on different monitors.



A good way to use dashboards is to use multiple monitors to display different widgets that show a comprehensive view of your network and security operations in real time. Select widgets that display information most relevant to you.

One scenario is to use the main monitors in the middle to display widgets in a bigger size. These widgets monitor network information that is most important to you. Then use the monitors on the sides to display other information in smaller widgets.

For example, use the top monitor in the middle to display the *Top Threat Destinations* widget in full screen, use the monitor(s) below that to display other *Security Monitor* widgets, use the monitors on the left to display *WiFi Monitor* widgets at the top and *System Performance* widgets at the bottom, and use the monitors on the right as a workspace to display widgets showing the busiest network activity. You can move, add, or remove widgets.

Using the NOC dashboard

NOC dashboards contains widgets that provide network and security information. Use the controls in the dashboard toolbar to work with a dashboard.

Add Widget	Add widgets to a predefined or custom dashboard. For details, see Customizing the NOC dashboard on page 108.
Dashboard	Create a new dashboard or reset a predefined dashboard to its default settings. For custom dashboards, you can rename or delete the custom dashboard. For details, see Customizing the NOC dashboard on page 108.
Create New	Create a new dashboard.
Reset	Reset the dashboard.
Select Security Fabric	Select the Security Fabric to display in the dashboard. You need to create a Security Fabric group in FortiGate and add the Security Fabric group in FortiAnalyzer to be able to select a Security Fabric option in the NOC dashboard.
Refresh	Refresh the data in the widgets.
Background color	Change the background color of the dashboard to make widgets easier to view in different room lighting. • *Day* shows a brighter gray background color. • *Night* shows a black background. • *Ocean* shows a blue background color.
Hide Side-menu and Show Side-menu	Hide or show the tree menu on the left.
Full Screen	Display in full screen. To exit full screen, press *Esc*.

Use the controls in the widget title bar to work with widgets.

Settings icon	Change the settings of the widget. Widgets have settings applicable to that widget, such as how many of the top items to display, *Time Period*, *Refresh Interval*, and *Chart Type*.
View different chart types	Some widget settings let you choose different chart types such as the *Disk I/O* and *Top Countries* widget. You can add these widgets multiple times and set each widget to show a different chart type.

Hide or show a data type	For widgets that show different data types, click a data type in the title bar to hide or show that data type in the graph. For example, in the *Insert Rate vs Receive Rate* widget, click *Receive Rate* or *Insert Rate* in the title bar to hide or show that data. In the *Disk I/O* widget, click *Read* or *Write* in the title bar to hide or show that data type.
Remove widget icon	Delete the widget from a predefined or custom dashboard.
Move widget	Click and drag a widget's title bar to move it to another location.
Resize widget	Click and drag the resize button in the bottom-right of the widget.
View more details	Hover the cursor over a widget's data points to see more details.
View a narrower time period	Some widgets have buttons below the graph. Click and drag the buttons to view a narrower time period.
Zoom in and out	For widgets that show information on a map such as the *Top Threat Destinations* widget, use the scroll wheel to change the zoom level. Click and drag the map to view a different area.

Customizing the NOC dashboard

You can add any widget to a predefined dashboard. You can also move, resize, or delete widgets. You cannot rename or delete a predefined dashboard. To reset a predefined dashboard to its default settings, click *Dashboard* > *Reset*.

You can add the same widget multiple times and configure each one differently, such as showing a different *Time Period*, *Refresh Interval*, or *Chart Type*.

To create a dashboard:

1. In the toolbar, click *Dashboard* > *Create New*.
2. Specify the *Name* and whether you want to create a blank dashboard or use a template.
   If you select *From Template*, specify which predefined dashboard you want to use as a template.
3. Click *OK*. The new dashboard appears In the tree menu.

To display Security Fabric in NOC:

1. Create a Security Fabric in FortiGate.
2. Add the Security Fabric in FortiAnalyzer.
3. Go to *NOC* > *Dashboard* > *Select Security Fabric*. The *Add Device* dialog box will open.
4. Select the Security Fabric you want to display in the NOC Dashboard.
5. Add desired widgets to the dashboard.

To add a widget:

1. Select the predefined or custom dashboard where you want to add a widget.
2. Click *Add Widget* to expand the menu; then locate the widget you want to add.

3. Click the + button to add widgets.
4. When you have finished adding widgets, click the close button to close the *Add Widget* pane.

NOC dashboards and widgets

NOC includes the following predefined dashboards and widgets. You can create custom dashboards and add any widget to any predefined or custom dashboard.

Security Monitor

The Security Monitor dashboard includes the following widgets:

Top Threat Destinations	A world map showing the highest network traffic. Hover the cursor over data points to see the source device and IP address, destination IP address and country, threat level, and the number of incidents (blocked and allowed).
Top Threat	The top threats to your network. Hover the cursor over data points to see the threat, category, threat level, threat score (blocked and allowed), and the number of incidents (blocked and allowed). The following incidents are considered threats: • Risk applications detected by application control • Intrusion incidents detected by IPS • Malicious web sites detected by web filtering • Malware/botnets detected by antivirus
Top Applications	The top applications used on the network. Hover the cursor over data points to see the application name, risk level, category, sessions (blocked and allowed), and bytes (sent and received).
Indicators of Compromise	Suspicious web use compromises. Hover the cursor over data points to see the end user IP address, host name, group, OS version, threat level, number of threats, and blacklist count.
Top Endpoint Vulnerabilities	Vulnerability information about FortiClient endpoints. Hover the cursor over data points to see the vulnerability count (critical, high, medium, and low), source IP address and device, and category.
Top Sources	The highest network traffic by source IP address and interface, sessions (blocked and allowed), threat score (blocked and allowed), and bytes (sent and received).
Top Countries	The highest network traffic by country, sessions (blocked and allowed), and bytes (sent and received). You can display this widget as a treemap chart, bubble chart, or bar chart; sorted by bandwidth or the number of sessions.
Security Fabric Score Summary	Total score and suggested actions to improve the score.

Historical Security Fabric Scores	Changes of the audit score over time.
Security Fabric Topology	A topology map showing the logical structure of connected security fabric devices.
Top Dialup VPN	A world map showing the users accessing the network using SSL or IPsec over a VPN tunnel. Hover the cursor over data points to see the user name or IP address, connected from IP address and country, connection time and duration, and bytes (sent and received).
VPN Site-to-Site	A world map showing the names of VPN tunnels with Internet protocol security (IPsec) that are accessing the network. Hover the cursor over data points to see the site-to-site IPsec tunnel, connected from and to IP address (including city and country if available), duration, and bytes (sent and received).
FortiSandbox - Scanning Statistics	The number of files scanned by FortiSandbox. This chart shows the files by type: malicious, suspicious, clean, and others. Hover the cursor over data points to see the number of files of each type.
FortiSandbox - Top Malicious & Suspicious File Users	Users or IP addresses that have the highest number of malicious and suspicious files detected by FortiSandbox. This chart shows the username and avatar if it's available, otherwise it shows the IP address. Hover the cursor over data points to see the number of files.

WiFi Monitor

The WiFi dashboard includes the following widgets:

Authorized APs	A world map showing the names of authorized WiFi access points on the network.
Top SSID	The top SSID (service set identifiers) of authorized WiFi access points on the network. Hover the cursor over data points to see the SSID and bytes (sent and received).
Top Rogue APs	The top SSID (service set identifiers) of unauthorized WiFi access points on the network. Hover the cursor over data points to see the SSID and total live time.

System Performance

The System Performance dashboard includes the following widgets:

CPU & Memory Usage	The usage status of the CPU and memory.
Multi-Core CPU Usage	The usage status of a multi-core CPU.

Insert Rate vs Receive Rate	The number of logs received vs the number of logs actively inserted into the database, including the maximum and minimum rates. • Receive rate: how many logs are being received. • insert rate: how many logs are being actively inserted into the database. If the insert rate is higher than the log receive rate, then the database is rebuilding. The lag is the number of logs waiting to be inserted.
Receive Rate vs Forwarding Rate	The number of logs received vs the number of logs forwarded out, including the maximum and minimum rates. • Receive rate: how many logs are being received. • Forward rate: how many logs are being forwarded out.
Disk I/O	The disk *Transaction Rate* (I/Os per second), *Throughput* (KB/s), or *Utilization* (%). The *Transaction Rate* and *Throughput* graphs also show the maximum and minimum disk activity.

Log View

You can view log information by device or by log group.

When rebuilding the SQL database, *Log View* is not available until the rebuild is complete. Click the *Show Progress* link in the message to view the status of the SQL rebuild.

When ADOMs are enabled, each ADOM has its own information displayed in *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 compressed log files.

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

Types of logs collected for each device

FortiAnalyzer 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 FortiAnalyzer collects from each type of device:

Device Type	Log Type
FortiAnalyzer	Event
FortiAuthenticator	Event
FortiGate	Traffic Security: Antivirus, Intrusion Prevention, Application Control, Web Filter, DNS, Data Leak Prevention, Email Filter, Web Application Firewall, Vulnerability Scan, VoIP, FortiClient Event: Endpoint, HA, Compliance, System, Router, VPN, User, WAN Opt. & Cache, WiFi
FortiCarrier	Traffic, Event, GTP
FortiCache	Traffic, Event, Antivirus, Web Filter
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 flowing through your FortiGate unit. Since traffic needs firewall policies to properly flow through FortiGate, this type of logging is also called firewall policy logging. Firewall policies control all traffic attempting to pass through the FortiGate unit, between FortiGate interfaces, zones, and VLAN sub-interfaces.

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.

DNS logs

DNS logs (FortiGate) record the DNS activity on your managed devices.

Event logs

Event logs record administration management and Fortinet device system activity, such as when a configuration changes, 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. FortiGate event logs includes *System*, *Router*, *VPN*, *User*, and *WiFi* menu objects to provide you with more granularity when viewing and searching log data.

The logs displayed on your FortiAnalyzer depends on the device type logging to it and the enabled features. 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*.

Log messages

You can view log information by device or by log group.

Viewing the log message list of a specific log type

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

To view the log message list:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Log View*, and select a log type from the tree menu.
   The corresponding log messages list is displayed.

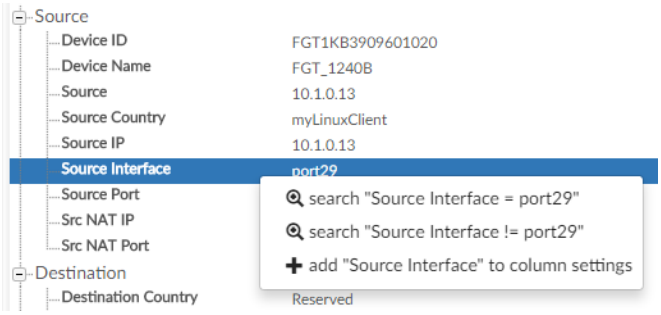
Viewing log message details

To view log message details:

1. Double-click a log message on the log message list.
   The log details pane is displayed to the right of the log message list, with the log fields categorized in tree view.

   You can display the log details pane below the log message list by clicking the *Bottom* icon in the log details pane. When the log details pane is displayed below the log message list, you can move it to the right of the log message list by clicking the *Right* icon. This is sometimes referred to as docking the pane to the bottom or right of the screen.

The log details pane provides shortcuts for adding filters and for showing or hiding a column. Right-click a log field to select an option.



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 toolbar of the log message list view, click *Column Settings* and select a column to hide or display.
   The available columns vary depending on the device and log type.
2. To add other columns, click *More Columns*. In the *Column Settings* dialog box, select the columns to show or hide.
3. To reset to the default columns, click *Reset to Default*.
4. Click *OK*.

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 title and move a column by drag and drop.

Filtering log messages

You can apply filters to the message list. Filters are not case-sensitive by default. If available, select *Tools* > *Case Sensitive Search* to create case-sensitive filters.

Filtering messages using filters in the toolbar

1. Go to the view you want.

Regular search	Click *Add Filter* and select a filter from the dropdown list, then type a value. Only displayed columns are available in the dropdown list. You can use search operators in regular search.
Switching between regular search and advanced search	At the right end of the *Add Filter* box, click the *Switch to Advanced Search* icon or click the *Switch to Regular Search* icon.
Advanced search	In Advanced Search mode, enter the search criteria (log field names and values).
Search operators and syntax	If available, click at the right end of the *Add Filter* box to view search operators and syntax. See also Search operators and syntax on page 117.

CLI string "freestyle" search	Searches the string within the indexed fields configured using the CLI command: `config ts-index-field`.
	For example, if the indexed fields have been configured using these CLI commands:
	`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 *Add Filter* box, FortiAnalyzer searches 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`.

2. In the toolbar, make other selections such as devices, time period, which columns to display, etc.

Filtering messages using the right-click menu

In a log message list, right-click an entry and select a filter criterion. The search criterion with a icon returns entries matching the filter values, while the search criterion with a icon returns entries that do not match the filter values.

Depending on the column in which your cursor is placed when you right-click, *Log View* uses the column value as the filter criteria. This context-sensitive filter is only available for certain columns.

To see log field name of a filter/column, right-click the column of a log entry and select a context-sensitive filter. The *Add Filter* box shows log field name.

Context-sensitive filters are available for each log field in the log details pane. See Viewing log message details on page 114.

Filtering messages using smart action filters

For *Log View* windows that have an *Action* column, the *Action* column displays smart information according to policy (log field action) and utmaction (UTM profile action).

The *Action* column displays a green checkmark *Accept* icon when both policy and UTM profile allow the traffic to pass through, that is, both the log field action and UTM profile action specify *allow* to this traffic.

The *Action* column displays a red X *Deny* icon and the reason when either the log field action or UTM profile action deny the traffic.

If the traffic is denied due to policy, the deny reason is based on the policy log field action.

If the traffic is denied due to UTM profile, the deny reason is based on the FortiView `threattype` from `craction`. `craction` shows which type of threat triggered the UTM action. The `threattype`, `craction`, and `crscore` fields are configured in FortiGate in Log & Report. For more information, see the *FortiOS - Log Message Reference* in the *Fortinet Document Library*.

A filter applied to the *Action* column is always a smart action filter.

The smart action filter uses the FortiGate UTM profile to determine what the *Action* column displays. If the FortiGate UTM profile has set an action to *allow*, then the *Action* column will display that line with a green *Accept* icon, even if the `craction` field defines that traffic as a threat. The green *Accept* icon does not display any explanation.

In the scenario where the `craction` field defines the traffic as a threat but the FortiGate UTM profile has set an action to *allow*, that line in the Log View *Action* column displays a green *Accept* icon. The green *Accept* icon does not display any explanation.

Search operators and syntax

Operators or symbols	Syntax
And	Find log entries containing all the search terms. Connect the terms with a space character, or “and”. Examples: 1. `user=henry group=sales` 2. `user=henry and group=sales`
Or	Find log entries containing any of the search terms. Separate the terms with “or” or a comma “,”. 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. Example: `-user=henry`
>, <	Find log entries greater than or less than a value, or within a range. This operator only applies to integer fields. Example: `policyid>1 and policyid<10`

Operators or symbols	Syntax
IP subnet/range search	Find log entries within a certain IP subnet or range. 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. Examples: 1. `srcip=192.168.1.*` 2. `policyid=1*` 3. `user=*`

Filtering FortiClient log messages in FortiGate traffic logs

For FortiClient endpoints 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=*`. A list of FortiGate traffic logs 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, *Log View* displays historical logs. *Custom View* and *Chart Builder* are only available in historical log view.

To view real-time logs, in the log message list view toolbar, click *Tools* > *Real-time Log*.

To switch back to historical log view, click *Tools* > *Historical Log*.

Viewing raw and formatted logs

By default, *Log View* displays formatted logs. The log view you select affects available view options. You cannot customize columns when viewing raw logs.

To view raw logs, in the log message list view toolbar, click *Tools* > *Display Raw*.

To switch back to formatted log view, click *Tools* > *Formatted Log*.

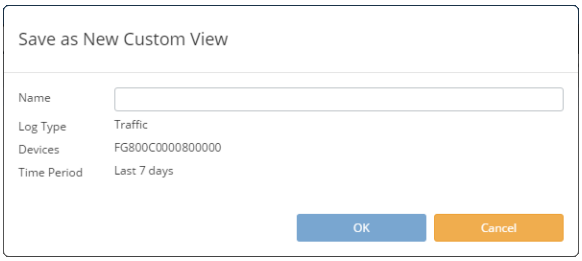
For more information about FortiGate raw logs, see the *FortiGate Log Message Reference* in the Fortinet Document Library. For more information about raw logs of other devices, see the *Log Message Reference* for the platform type.

Custom views

Use *Custom View* to save the filter setting, device selection, and the time period you have specified.

To create a new custom view:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Log View*, and select a log type.
3. In the content pane, customize the log view as needed by adding filters, specifying devices, and/or specifying a time period.
4. In the toolbar, click *Custom View*.



5. In the *Name* field, type a name for the new custom view.
6. Click *OK*. The custom view is now displayed under *Log View* > *Custom View*.

To edit a custom view:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to the *Log View* > *Custom View*.
3. In the toolbar, edit the filter settings, and click *GO*.
4. In the toolbar, click *Custom View*.
5. Click *Save* to save the changes to the existing custom view or click *Save as* to save the changes to a new custom view.
6. Click *OK*.

To view the traffic log of a custom view:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to the *Log View* > *Custom View*.
3. Right-click the name of a custom view and select *View Traffic*.

Downloading log messages

You can download historical log messages to the management computer as a text or CSV file. You cannot download real-time log messages.

To download log messages:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Log View*, and select a log type.
3. In the toolbar, click *Tools* > *Download*.
4. In the *Download Logs* dialog box, configure download options:
   - In the *Log file format* dropdown list, select *Text* or *CSV*.
   - To compress the downloaded file, select *Compress with gzip*.

- To download only the current log message page, select *Current Page*. To download all the pages in the log message list, select *All Pages*.

5. Click *Download*.

Creating charts

You can also create charts in *Reports* > *Report Definitions* > *Chart Library*. See Chart library on page 160

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

To create charts with Chart Builder:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Log View*, and select a log type.
3. In the toolbar, click *Tools* > *Chart Builder*.
4. In the *Chart Builder* dialog box, configure the chart and click *Save*.

Name	Type a name for the chart.
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	Show Limit
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.

Log groups

You can group devices into log groups. You can view FortiView summaries, display logs, generate reports, or create handlers for a log group. Log groups are virtual so they do not have SQL databases or occupy additional disk space.

In FortiAnalyzer 5.0.6 and earlier, you can treat log groups as a single device that has its own SQL database. You cannot do this in FortiAnalyzer 5.2 and later.

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

To create a new log group:

1. Go to *Log View* > *Log Group*.
2. In the content pane toolbar, click *Create New*.
3. In the *Create New Log Group* dialog box, type a log group name and add devices to the log group.
4. Click *OK*.

Log browse

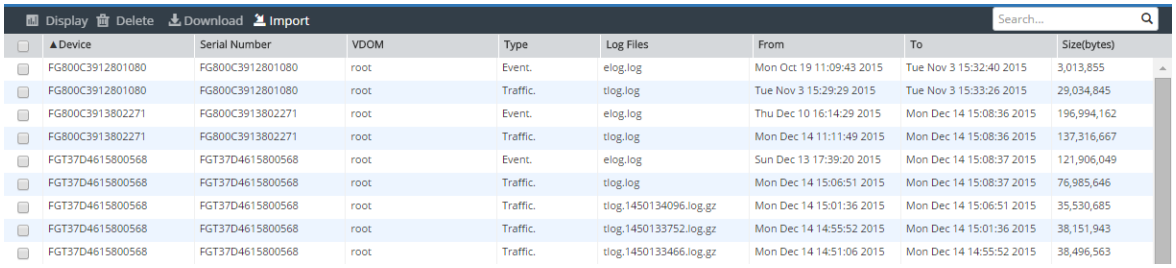
When a log file reaches its maximum size or a scheduled time, FortiAnalyzer rolls the active log file by renaming the file. The file name is in the form of `xlog.N.log`, where `x` is a letter indicating the log type, and `N` is a unique number corresponding to the time the first log entry was received. For information about setting the maximum file size and log rolling options, see Device logs on page 217.

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

In Collector mode, if you want to view the latest log messages, select the latest log file to display its log messages.

To view log files:

1. Go to *Log View* > *Log Browse*
2. Select a log file, and click *Display* 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 114.



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.

Log files can also be imported into a different FortiAnalyzer unit. Before importing the log file you must add all devices included in the log file to the importing FortiAnalyzer.

To insert imported logs into the SQL database, the `config system sqlstart-time` and `rebuild-event-start-time` must be **older** than the date of the logs that are imported **and** the storage policy for analytic data (the *Keep Logs for Analytics* field) must also extend back far enough.

To set the SQL start time and rebuild event start time using CLI commands:

```
config system sql
   set start-time <start-time-and-date>
   set rebuild-event-start-time <start-time-and-date>
end
```

Where `<start-time-and-date>` is in the format `hh:mm yyyy/mm/dd`.

To import a log file:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Log View* > *Log Browse* and click *Import* in the toolbar.
3. In the *Device* dropdown list, select the device the imported log file belongs to or select *[Take From Imported File]* to read the device ID from the log file.
   If you select *[Take From Imported File]*, the log file must contain a `device_id` field in its log messages.
4. Drag and drop the log file onto the dialog box, or click *Add Files* and locate the file to be imported on your local computer.
5. Click *OK*. A message appears, stating that the upload is beginning, but will be canceled if you leave the page.
6. Click *OK*. The upload time varies depending on the size of the file and the speed of the connection.
   After the log file is successfully uploaded, FortiAnalyzer inspects the file:
   - If the `device_id` field in the uploaded log file does not match the device, the import fails. Click *Return* to try again.
   - If you selected *[Take From Imported File]* and the FortiAnalyzer unit's device list does not currently contain that device, an error is displayed stating *Invalid Device ID*.

Downloading a log file

You can download a log file to save it as a backup or to 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* and select the log file that you want to download.
2. In the toolbar, click *Download*.

3. In the *Download Log File(s)* dialog box, configure download options:
   - In the *Log file format* dropdown list, select *Native*, *Text*, or *CSV*.
   - If you want to compress the downloaded file, select *Compress with gzip*.
4. Click *Download*.

Deleting log files

To delete log files:

1. Go to *Log View* > *Log Browse*.
2. Select one or more files and click *Delete*.
3. Click *OK* to confirm.

Event Management

Event Management displays all events generated by event handlers.

How ADOMs affect events

When ADOMs are enabled, each ADOM has its own event handlers and lists of events. Ensure you are in the correct ADOM before viewing *Event Management*. See Switching between ADOMs on page 25.

Predefined event handlers

You can use predefined event handlers to generate events for *Event Management*. There are predefined event handlers for FortiGate and FortiCarrier devices. For other devices, you can create custom event handlers.

Logs used for events

Event Management displays events from Analytics logs, not Archive logs. 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 Management. You must enable an event handler to start generating events. To see which event handlers are enabled or disabled, see Enabling event handlers on page 132.

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

Managing event handlers

To manage event handlers, go to *Event Management* > *Event Handler List*. The following options are available:

Option	Description
Create New	Create a new event handler.

Option	Description
Edit	Edit the selected event handler.
Delete	Delete the selected event handler. You cannot delete predefined event handlers.
Clone	Clone the selected 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.
Collapse All / Expand All	Collapse or expand the *Filters* column.
Show Predefined	Show or hide predefined handlers in the list.
Show Custom	Show or hide custom handlers in the list.
Factory Reset	If you have modified a predefined event handler, return the selected predefined event handler to its factory default settings.

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	Enabled by default • Severity: Medium • Log Type: Traffic • Event Category: Antivirus • Group by: Virus Name • Log messages that match all conditions: • *Level Greater Than or Equal To Information* • Generic Text Filter: `virus!='' and virus!='N/A'`

App Ctrl Event	Enabled by default
	• Severity: Critical
	• Log Type: Traffic
	• Event Category: Application Control
	• Group by: Application Name
	• Log messages that match any of the following conditions:
	  • *Application Category Equal To Botnet*
	  • *Application Category Equal To Proxy*

Event Handler	Description

Application Crashed Event	Enabled by default
	• Severity: Medium
	• Log Type: Event Log
	• Event Category: System
	• Group by: Log Description
	• Log messages that match all conditions:
	  • *Log Description Equal To Application crashed*
	  • *Level Greater Than or Equal To Warning*

Botnet Application Allowed by Application Control	Disabled by default
	• Severity: Critical
	• Log Type: Application Control
	• Group by: Application Name
	• Log messages that match all of the following conditions:
	  • *Application Category Equal to Botnet*
	  • *(action==pass or action==monitor)*

Botnet Application Blocked by Application Control	Disabled by default
	• Severity: High
	• Log Type: Application Control
	• Group by: Application Name
	• Log messages that match all of the following conditions:
	  • *Application Category Equal to Botnet*
	  • *Action Not Equal to Pass*
	  • *Action Not Equal to Monitor*

Botnet C-and-C Allowed by IP-Reputation	Disabled by default
	• Severity: High
	• Log Type: Application Control
	• Group by: Virus Name
	• Log messages that match all of the following conditions:
	  • *Action Not Equal to Blocked*
	  • *logid==0202009248 or logid==0202009249*

Botnet C-and-C Blocked by DNS Filtering	Disabled by default
	• Severity: Medium
	• Log Type: DNS
	• Group by: Message
	• Log messages that match all of the following conditions:
	  • *Level Greater Than or Equal to Information*
	  • *logid==1501054600 or logid==1501054601*

Event Handler	Description

Botnet C-and-C Blocked by IP-Reputation	Disabled by default
	• Severity: Medium
	• Log Type: AntiVirus
	• Group by: Virus Name
	• Log messages that match all of the following conditions:
	  • *Action Equal to Blocked*
	  • *logid==0202009248 or logid==0202009249*

Botnet Traffic Allowed by IPS	Disabled by default
	• Severity: Critical
	• Log Type: IPS
	• Group by: Attack Name
	• Log messages that match all of the following conditions:
	  • *Level Greater Than or Equal To Information*
	  • *attack ~ Botnet and (action=='detected' or action=='pass session')*

Botnet Traffic Blocked by IPS	Disabled by default
	• Severity: High
	• Log Type: IPS
	• Group by: Attack Name
	• Log messages that match all of the following conditions:
	  • *Level Greater Than or Equal To Information*
	  • *attack ~ Botnet and (action!='detected' or action!='pass session')*

Conserve Mode	Disabled by default • Severity: Critical • Log Type: Event • Event Category: System • Group by: Message • Log messages that match all conditions: • *Log Description Equal To System services entered conserve mode*
DLP Event	Disabled by default • Severity: Medium • Log Type: Traffic Log • Event Category: DLP • Group by: DLP Rule Name • Log messages that match all conditions: • *Security Action Equal To Blocked*

Event Handler	Description
DNS Botnet C-and-C - High Severity	Enabled by default • Severity: High • Log Type: DNS • Group by: Message • Log messages that match all conditions: • *Level Equal To Warning* • Generic Text Filter: `botnetip!='' or botnetdomain!=''`

HA Failover	Disabled by default
	• Severity: Medium
	• Log Type: Event Log
	• Event Category: HA
	• Group by: Log Description
	• Log messages that match any of the following conditions:
	  • *Log Description Equal To Virtual cluster move member*
	  • *Log Description Equal To Virtual cluster member state moved*

Interface Down	Disabled by default
	• Severity: High
	• Log Type: Event Log
	• Event Category: System
	• Group by: Message
	• Log messages that match all conditions:
	  • *Action Equal To interface-stat-change*
	  • *Status Equal To DOWN*

Interface Up	Disabled by default
	• Severity: Medium
	• Log Type: Event Log
	• Event Category: System
	• Group by: Message
	• Log messages that match all conditions:
	  • *Action Equal To interface-stat-change*
	  • *Status Equal To UP*

IPS - Critical Severity	Enabled by default • Severity: Critical • Log Type: IPS • Group by: Attack Name • Log messages that match all conditions: • *Severity Equal To Critical*

Event Handler	Description
IPS - High Severity	Enabled by default • Severity: High • Log Type: IPS • Group by: Attack Name • Log messages that match all conditions: • *Severity Equal To High*
IPS - Low Severity	Disabled by default • Severity: Low • Log Type: IPS • Group by: Attack Name • Log messages that match all conditions: • *Severity Equal To Low*
IPS - Medium Severity	Disabled by default • Severity: Medium • Log Type: IPS • Group by: Attack Name • Log messages that match all conditions: • *Severity Equal To Medium*
IPsec Phase2 Down	Disabled by default • Severity: Medium • Log Type: Event Log • Event Category: VPN • Group By: VPN Tunnel • Log messages that match all conditions: • *Action Equal To phase2-down*
IPsec Phase2 Up	Disabled by default • Severity: Medium • Log Type: Event Log • Event Category: VPN • Group By: VPN Tunnel • Log messages that match all conditions: • *Action Equal To phase2-up*

Event Handler	Description
Local Device Event	Found only in the Root ADOM. Enabled by default • Devices: Local Device • Severity: Medium • Log Type: Event Log • Event Type: Any • Group By: Device ID • Log messages that match any of the following conditions: • *Level Equal To Emergency*

Malware Traffic Allowed By AntiVirus	Disabled by default
	• Severity: High
	• Log Type: AntiVirus
	• Group By: Virus Name
	• Log messages that match all conditions:
	  • *Level Greater Than or Equal to Information*
	  • *logid==0211008193 or logid==0211008195*

Malware Traffic Allowed by FortiSandbox	Disabled by default
	• Severity: High
	• Log Type: AntiVirus
	• Group By: Virus Name
	• Log messages that match all conditions:
	  • *Level Greater Than or Equal to Information*
	  • *logid==0211009235 or logid==0211009237*

Malware Traffic Blocked by AntiVirus	Disabled by default
	• Severity: Medium
	• Log Type: AntiVirus
	• Group By: Virus Name
	• Log messages that match all conditions:
	  • *Level Greater Than or Equal to Information*
	  • *logid==0211008192 or logid==0211008194*

Malware Traffic Blocked by FortiSandbox Signature Update	Disabled by default
	• Severity: Medium
	• Log Type: AntiVirus
	• Group By: Virus Name
	• Log messages that match all conditions:
	  • *Level Greater Than or Equal to Information*
	  • *logid==0211009234 or logid==0211009236*

Event Handler	Description

Power Supply Failure	Disabled by default
	• Severity: Critical
	• Log Type: Event Log
	• Event Category: System
	• Group by: Message
	• Log messages that match all conditions:
	  • *Action Equal To power-supply-monitor*
	  • *Status Equal To failure*

UTM Antivirus Event	Enabled by default • Severity: High • Log Type: Antivirus Log • Group by: Virus Name • Log messages that match all conditions: • *Level Greater Than or Equal To Information* • Generic Text Filter: `virus!='' and virus!='N/A' and dtype!='fortisandbox'`

UTM App Ctrl Event	Enabled by default
	• Severity: Critical
	• Log Type: Application Control
	• Group by: Application Name
	• Log messages that match any of the following conditions:
	  • *Application Category Equal To Botnet*
	  • *Application Category Equal To Proxy*

UTM DLP Event	Disabled by default • Severity: Medium • Log Type: DLP • Group by: Profile • Log messages that match all conditions: • *Action Equal To Block*

Event Handler	Description

UTM Web Filter Event	Enabled by default
	• Severity: Medium
	• Log Type: Web Filter
	• Group by: Category
	• Log messages that match any of the following conditions:
	  • *Web Category Equal To Child Abuse*
	  • *Web Category Equal To Discrimination*
	  • *Web Category Equal To Drug Abuse*
	  • *Web Category Equal To Explicit Violence*
	  • *Web Category Equal To Extremist Groups*
	  • *Web Category Equal To Hacking*
	  • *Web Category Equal To Illegal or Unethical*
	  • *Web Category Equal To Plagiarism*
	  • *Web Category Equal To Proxy Avoidance*
	  • *Web Category Equal To Malicious Websites*
	  • *Web Category Equal To Phishing*
	  • *Web Category Equal To Spam URLs*

Web Filter Event	Enabled by default
	• Severity: Medium
	• Log Type: Traffic Log
	• Event Category: Web Filter
	• Group by: Category
	• Log messages that match any of the following conditions:
	  • *Web Category Equal To Child Abuse*
	  • *Web Category Equal To Discrimination*
	  • *Web Category Equal To Drug Abuse*
	  • *Web Category Equal To Explicit Violence*
	  • *Web Category Equal To Extremist Groups*
	  • *Web Category Equal To Hacking*
	  • *Web Category Equal To Illegal or Unethical*
	  • *Web Category Equal To Plagiarism*
	  • *Web Category Equal To Proxy Avoidance*
	  • *Web Category Equal To Malicious Websites*
	  • *Web Category Equal To Phishing*
	  • *Web Category Equal To Spam URLs*

Enabling event handlers

For both predefined and custom event handlers, you must enable the event handler to generate events. In the *Event Handler List*, the *Name* column displays a  icon for enabled event handlers and a  icon for disabled event

handlers.

If you want to receive alerts for predefined events handlers, edit the predefined event handler to configure notifications.

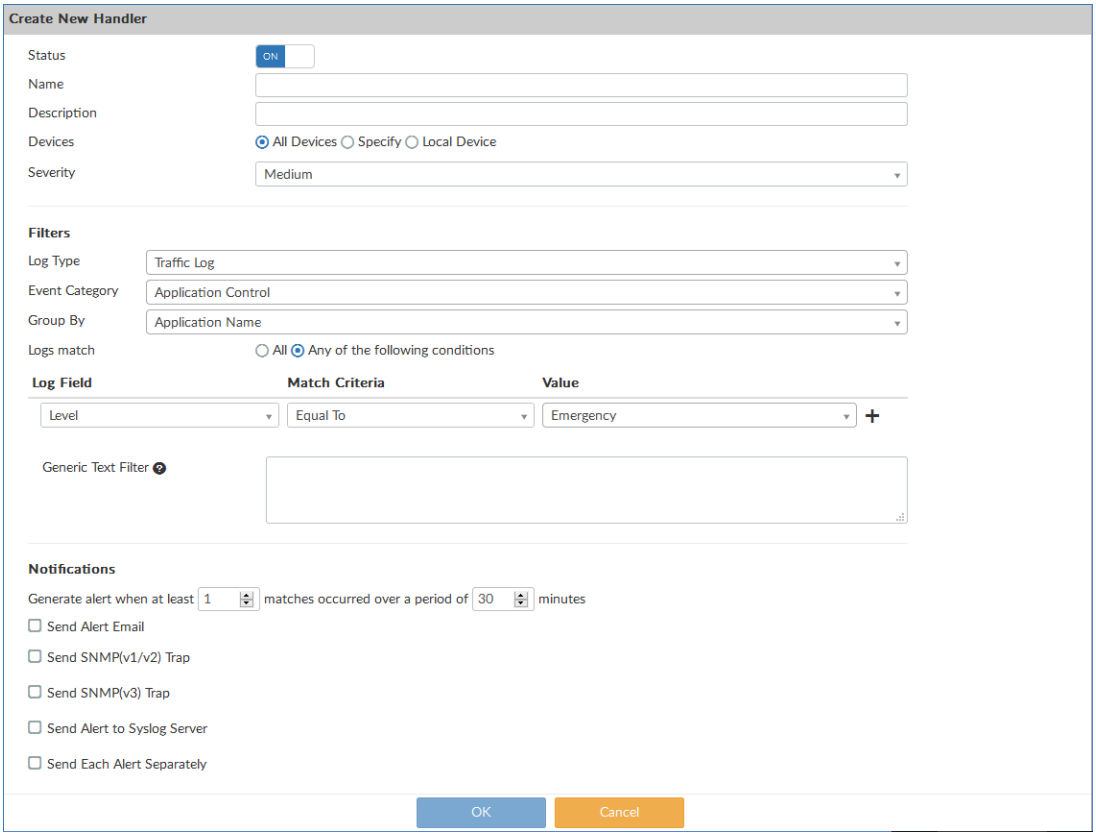
To enable event handlers:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Event Management* > *Event Handler List*.
3. Select one or more event handlers and click *More* > *Enable* or right-click an event handler and select *Enable*.

Creating custom event handlers

To create a new event handler:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Event Management* > *Event Handler List*.
3. In the toolbar, click *Create New*.



4. Configure the settings as required and click *OK*. For a description of the fields, see Create New Handler pane on page 134.
5. Click *OK* to create the new event handler.

Creating custom event handlers using the Generic Text Filter

The *Generic Text Filter* uses regex (regular expression) syntax. You must use an escape character when needed. For example, `cfgpath=firewall.policy` is the wrong syntax because it's missing an escape character. The correct syntax is `cfgpath=firewall\.policy`.

To create an event handler using the Generic Text Filter to match raw log data:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Log View*, and select a log type.
3. In the toolbar, click *Tools* > *Display Raw*.
   The easiest method is to copy the text string you want from the raw log and paste it into the *Generic Text Filter* field. Ensure you insert an escape character when necessary, for example, `cfgpath=firewall\.policy`.
4. Locate and copy the text in the raw log.
5. Go to *Event Management* > *Event Handler List* and click *Create New*.
6. In the *Generic Text Filter* box, paste the text you copied or type the text you want. Ensure you use the raw log field names, for example, `mem` (not memory) and `setuprate` (not setup-rate).
   For information on text format and operators, hover the cursor over the help icon. The operator `~` means contains and `!~` means does not contain.
7. If you want to be notified of events, configure the *Notifications* section.
8. Configure other settings as required and click *OK*. For a description of the fields, see Create New Handler pane on page 134.

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	Add a name for the handler.
Description	Type a description of the event handler.
Devices	Select the devices to include. • *All Devices*. • *Specify*: To add devices, click the Add icon. • *Local Device*: Select if the event handler is for local FortiAnalyzer event logs. This option is only available in the root ADOM and is used to query FortiAnalyzer event logs. For *Local Device*, the *Log Type* must be *Event Log* and *Event Category* must be *Any*.
Severity	Select the severity from the dropdown list: *Critical*, *High*, *Medium*, or *Low*.
Filters	Configure filters for the handler.

Field		Description
	Log Type	Select the log type from the dropdown list. When *Devices* is set to *Local Device*, you cannot change the *Log Type* or *Event Category*.
	Event Category	Select the category of event that this handler monitors. The available options depends on the platform type. This option is only available when *Log Type* is set to *Event Log* or *Traffic Log*.
	Group By	Select how to group the events.
	Logs match	Select *All* or *Any of the following conditions*.
	Log Field	Select a log field to filter from the dropdown list. The available options depends on the selected log type.
	Match Criteria	Select a match criteria from the dropdown list. The available options depends on the selected log field.
	Value	Either select a value from the dropdown list or enter a value in the text box. The available options depends on the selected log field.
	Add	Add log filter. When *Devices* is set to *Local Device* this option is not available. You can only have one log field filter.
	Remove	Delete the filter.
	Generic Text Filter	Enter a generic text filter. For more information on creating a generic text filter, see Creating custom event handlers using the Generic Text Filter on page 134. For information on text format, hover the cursor over the help icon. The operator ~ means contains and !~ means does not contain.
Notifications		Configure alerts for the handler.
	Generate alert when at least *n* matches occurred over a period of *n* minutes	Enter threshold values to generate alerts. Enter the number of matching events that must occur in the number of minutes to generate an alert.
	Send Alert Email	Send an alert by email. Specify email parameters including the mail server. For more information, see Mail Server on page 213.
	Send SNMP(...) Trap	Select one or both checkboxes and specify an SNMP community or user from the dropdown list. Click the add icon to create a new SNMP community or user. For more information, see SNMP on page 204.
	Send Alert to Syslog Server	Send an alert to the syslog server. Select a syslog server from the dropdown list. Click the add icon to create a new syslog server. For more information, see Syslog Server on page 215.

Field	Description
Send Each Alert Separately	Select to send each alert individually instead of in a group.

Filtering event handlers

You can filter the list of event handlers to show only predefined or custom handlers.

To filter event handlers:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Event Management* > *Event Handler List*.
3. In the toolbar, click *More* > *Show Predefined* or *More* > *Show Custom* to filter the event handlers.

Searching event handlers

To search event handlers:

1. Go to *Event Management* > *Event Handler List*.
2. Type a search term in the search box at the top-right.

Resetting to factory defaults

You can change predefined event handlers as needed. If required, you can restore predefined event handlers to factory default settings.

To reset predefined event handlers:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Event Management* > *Event Handler*.
3. Ensure the *Show Predefined* checkbox is selected.
4. Select one or more predefined event handlers.
5. Click *More* > *Factory Reset* to return the settings to factory defaults.

You can also reset predefined event handlers to factory default settings in the *Edit Handler* page.

Events

After event handlers start generating events, you can view events and event details. *Event Management* > *All Events* shows events by type and severity in a graphical format, and recent events in a tabular format. *Event Management* > *Calendar View* shows events by month or week in a calendar or bar chart format.

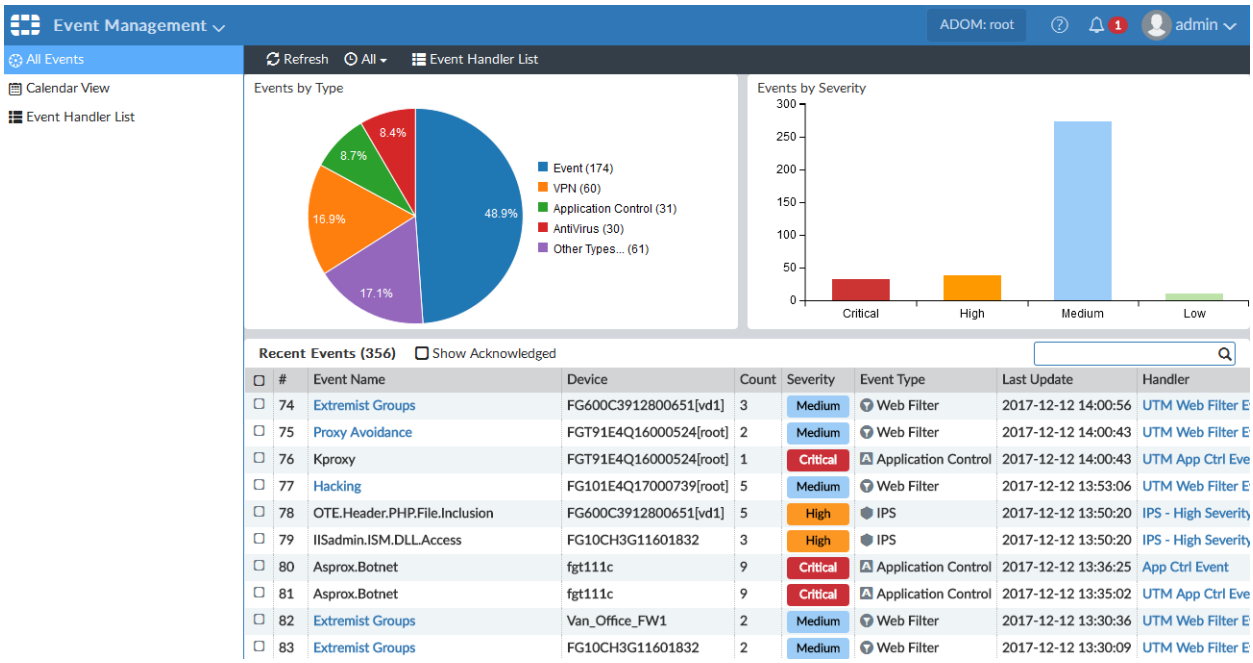
When rebuilding the SQL database, you might not see a complete list of historical events. However, you can always see events in real-time logs. You can view the status of the SQL rebuild by checking the *Rebuilding DB* status in the *Notification Center*.

Event summaries

- To view event summaries, go to *Event Management* > *All Events*.
- To manually refresh the event summaries data, click *Refresh*.

  You can automatically set the refresh interval to *Every 10 Seconds*, *Every 30 Seconds*, *Every 1 Minute*, or *Every 5 Minutes*.
- To change the time period to display, click the time icon and specify a time period.
- To view event handlers, click *Event Handler List* (see Event handlers on page 124).

All Events show events by type and severity in a graphical format, and recent events in a tabular format.



Events by Type	*Events by Type* shows a pie chart organized by event type. • To view the number of alerts (*Events*) and the number of logs (*Counts*) for that event type, hover the cursor over parts of the pie or legend. • To view a list showing only that type of event, click on that element in the chart.

Events by Severity	*Events by Severity* shows a bar chart organized by event severity. • To view the number of alerts (*Events*) and the number of logs (*Counts*) for that event severity, hover the cursor over a bar. • To view a list showing only events with that severity, click on a bar in the chart.
Recent Events	*Recent Events* shows events for the selected time span. • To sort by a column, click the column header. • To include acknowledged events, click *Show Acknowledged*. See Acknowledging events. • To search the list, type a search term in the search box. • To edit a handler, click a *Handler* element. See Event handlers. • To view information about an event and recommended actions, click its *Event Name* hyperlink. This option is only available for some events. • To view event details, double-click the event line. See Event details.

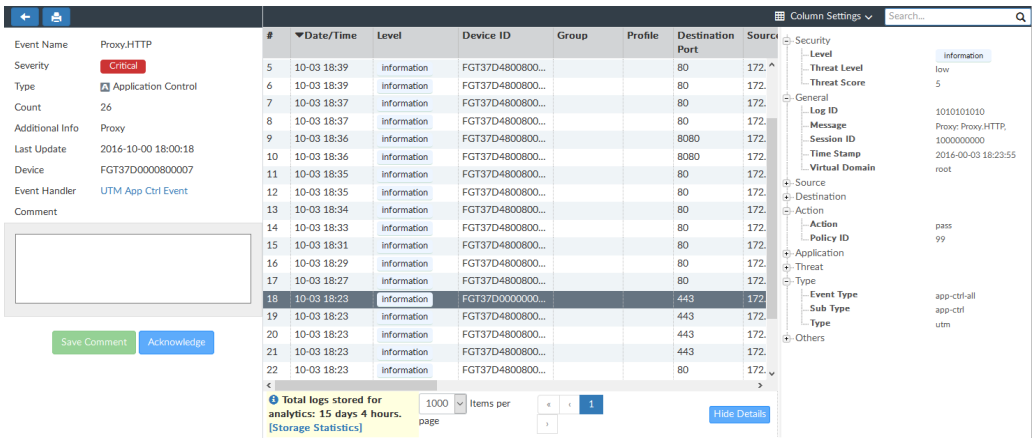
Filtered event list

In *Events by Type* and *Events by Severity*, click an element to show only events of that type or severity. The filtered event list shows the same information and options as the *Recent Events* list.

To return to the previous page, click the back button.

Event details

In *Recent Events* or a filtered events list, to view event details, double-click the event line or right-click the event and select *View Details*.



The event details page contains information about the event and a list of all individual logs. You can print, acknowledge, and add comments to the event.

- To change what columns to display, click *Column Settings* or *Column Settings* > *More Columns*.
- To display more details, double-click a line or select a line and click *Display Details* in the bottom-right. The log details pane open on the right side of the window.
- To return to the previous page, click the back button.

Acknowledging events

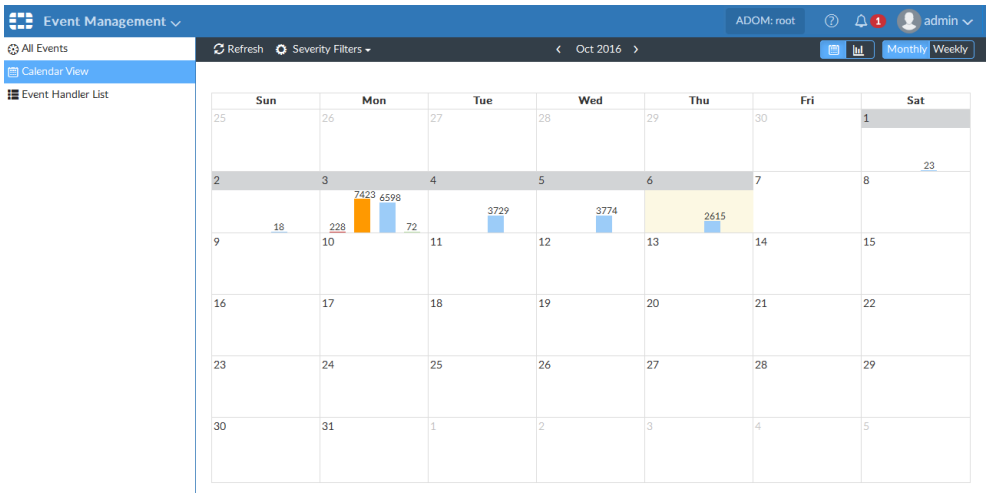
Acknowledging an event removes it from the recent events list (if *Show Acknowledged* is not selected).

To acknowledge events:

- In the recent events list, select one or more events, then right-click and select *Acknowledge*.
- In the event details page, click *Acknowledge*.

Event calendar

Calendar View shows events by month or week in a calendar or bar chart format.

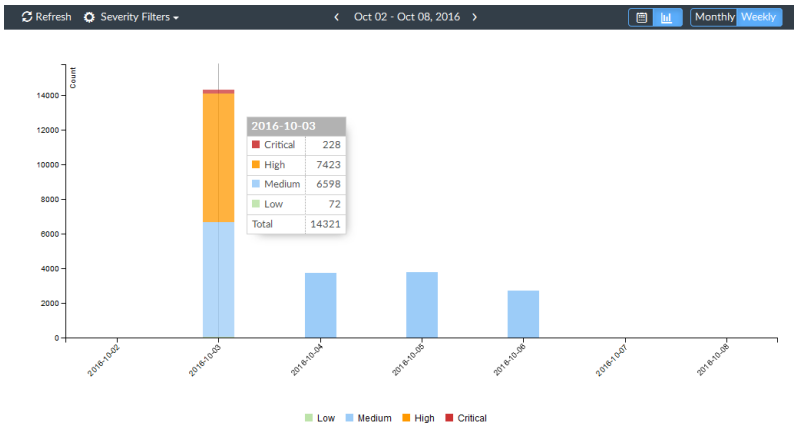


To include only events of a specific severity, click *Severity Filters* and select which severity levels to include. The default filter is critical and high severity.

Click on any element in any of the views to open the filtered events list; see Filtered event list on page 138.

Click the *Calendar Chart* button in the toolbar to display the calendar. The monthly view of the calendar shows bar charts of the events by severity on each day of the month. The weekly view shows the events for each hour of each day of the week. Click the arrows on either side of the calendar heading to scroll through months or weeks.

Click the *Bar Chart* button in the toolbar to change to the bar chart view. The bar chart view shows a stacked, vertical bar chart of the count versus time (days). Hovering the cursor over a bar shows the number of logs of each severity and the total for that day.


Refresh
Severity Filters
Oct 02 - Oct 08, 2016
Monthly
Weekly
Count
14000
12000
10000
8000
6000
4000
2000
0
2016-10-03
Critical 228
High 7423
Medium 6598
Low 72
Total 14321
2016-10-02
2016-10-03
2016-10-04
2016-10-05
2016-10-06
2016-10-07
2016-10-08
Low
Medium
High
Critical

Reports

You can generate data reports from logs by using the *Reports* feature. You can do the following:

- Use predefined reports. Predefined report templates, charts, and macros are available to help you create new reports.
- Create customize reports.

Report files are stored in the reserved space for the FortiAnalyzer device. See Automatic deletion on page 88.

When rebuilding the SQL database, *Reports* are not available until 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 you are in the correct ADOM before selecting a report. See Switching between ADOMs on page 25.

Some reports are available only when ADOMs are enabled. For example, ADOMs must be enabled to access FortiCarrier, FortiCache, FortiClient, FortiDDoS, FortiMail, FortiSandbox, and FortiWeb reports. 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 you can use to create and/or build reports.

Predefined...	GUI Location	Purpose
Reports	*Reports* > *Report Definitions* > *All Reports*	You can generate reports directly or with minimum setting configurations. Predefined reports are actually report templates with basic default setting configurations.
Templates	*Reports* > *Report Definitions* > *Templates*	You can 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 158.
Charts	*Reports* > *Report Definitions* > *Chart Library*	You can use directly or build upon a report template 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*	You can use directly or build upon 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.

For reports about users, the FortiGate needs to populate the `user` field in the logs sent to FortiAnalyzer. For more information see the *FortiOS Handbook* > *Authentication* > *Configuring authenticated access* and *Agent-based FSSO*.

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. Each chart requires a specific log type.

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*. The *hcache* (hard cache) means that 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 for the same SQL query, so *hcache* is used. *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.

The *auto-cache* process uses system resources to assemble and cache the datasets and 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

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 147 and Creating charts on page 160 and Macro library on page 163.
4. In the toolbar, click *Run Report*.

Viewing completed reports

After you generate reports, you can view completed reports in *Reports* > *Generated Reports* or *Reports* > *Report Definitions* > *All Reports*. You can view reports in the following formats: HTML, PDF, XML, and CSV.

To view completed reports in Generated Reports:

1. Go to *Reports* > *Generated Reports*.
   This view shows all generated reports for the specified time period.
2. To sort the report list by date, click *Order by Time*.To sort the report list by report name, click *Order by Name*.
3. Locate the report and click 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.

To view completed reports in All Reports:

1. Go to *Reports* > *Report Definitions* > *All Reports*.
2. On the report list, double-click a report to open it.
3. In the *View Report* tab, locate the report and click 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 142.

You can see the status of building the cache in *Reports* > *Report Definitions* > *All Reports* in the *Cache Status* column.

To enable auto-cache:

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

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. Grouping reports has these advantages:

- Reduce the number of *hcache* tables.
- Improve *auto-hcache* completion time.
- Improve report completion time.

Step 1: Configure report grouping

For example, 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:

- The `report-like` field specifies the string in report titles that is used for report grouping. This string is case-sensitive.
- The `group-by` value controls how cache tables are grouped.
- To view report grouping information, enter the following CLI command, then check the Report Group column of the table that is displayed.
  `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 hcache rebuild-report <start-time> <end-time>
```

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

Retrieving report diagnostic logs

Once you start to run a report, FortiAnalyzer creates a log about the report generation status and system performance. Use this diagnostic log to troubleshoot report performance issues. For example, if your report is very slow to generate, you can use this log to check system performance and see which charts take the longest time to generate.

For information on how to interpret the report diagnostic log and troubleshoot report performance issues, see the *FortiAnalyzer Report Performance Troubleshooting Guide*.

To retrieve report generation logs:

1. In *Reports* > *Generated Report*, right-click the report and select *Retrieve Diagnostic* to download the log to your computer.
2. Use a text editor to open the log.

Auto-Generated Reports

The *Cyber Threat Assessment* report is automatically generated. By default, the report will run at 3:00AM every Monday. For more information on report scheduling, see Scheduling reports on page 145.

Schedules can be viewed in the *Report Calendar*. See "Report calendar" on page 171.

This will only affect newly installed FortiAnalyzer or newly created ADOM. Upgraded ADOM reports, scheduling and calendar will be kept as is.

Scheduling reports

You can configure a report to generate on a regular schedule. Schedules can be viewed in the *Report Calendar*. See Report calendar on page 171.

To schedule a report:

1. Go to *Reports* > *Report Definitions* > *All Reports*.
2. Select a report and click *Edit* in the toolbar.
3. Click *Settings* in the toolbar.
4. Select the *Enable Schedule* checkbox and configure the schedule.
5. Click *Apply*.

Creating reports

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

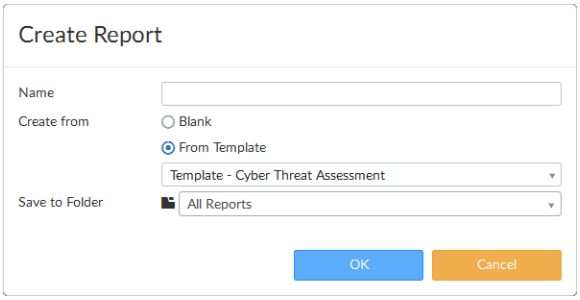
Creating reports from report templates

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. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.

3. In the toolbar, click *Create New*. The *Create Report* dialog box opens.



4. In the *Name* box, type a name for the new report. The following characters are NOT supported in report names: \ / " ' < > & , | # ? % $ +
5. Select *From Template* for the *Create from* setting, then select a template from the dropdown list. The template populates the *Layout* tab of the report.
6. Select the folder that the new report will be saved to from the dropdown list. See Organizing reports into folders on page 155 for information about folders.
7. Select *OK* to create the new report.
8. On the *Settings* tab, configure the settings as required. For a description of the fields, see Reports Settings tab on page 147.
9. Optionally, go to the *Layout* tab to customize the report layout and content. For a description of the fields, see Reports Layout tab on page 150.
10. Click *Apply* to save your changes.

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. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. In the content pane, select the report from the list, then click *Clone* in the toolbar.
4. In the *Clone Report* dialog box, type a name for the cloned report. The following characters are NOT supported in report names: \ / " ' < > & , | # ? % $ +
5. Select the folder that the new report will be saved to from the dropdown list. See Organizing reports into folders on page 155 for information about folders.
6. Select *OK* to create the new report.
7. On the *Settings* tab, configure the settings as required. For a description of the fields, see Reports Settings tab on page 147.
8. Optionally, go to the *Layout* tab to customize the report layout and content. For a description of the fields, see Reports Layout tab on page 150.
9. Click *Apply* to save your changes.

Creating reports without using a template

To create a report without using a template:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. In the toolbar, click *Create New*. The *Create New Report* dialog box opens.
4. In the *Name* box, type a name for the new report. The following characters are NOT supported in report names: \ / " ' < > & , | # ? % $ +
5. Select the *Blank* option for the *Create from* setting.
6. Select the folder that the new report will be saved to from the dropdown list. See Organizing reports into folders on page 155 for information about folders.
7. Select *OK* to create the new report.
8. 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 147.

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

9. 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 Layout tab on page 150.

   For information about creating charts and macros, see Creating charts on page 160 and Creating macros on page 163.
10. Click *Apply* to save your changes.

Reports Settings tab

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

Field	Description
Time Period	The time period the report covers. Select a time period or select *Custom* to manually specify the start and end date and time.
Devices	The devices to include in the report. 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)*. This option is only available if multiple devices are selected.
Enable Schedule	Select to enable report template schedules.

Field	Description
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. Enter a number for the frequency of the report based on the time period selected from the dropdown 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 to never ending.
Enable Notification	Select to enable report notification.
Output Profile	Select the output profile from the dropdown list, or click *Create New* to create a new output profile. See Output profiles on page 168.

Filters section of Reports Settings tab

See Filtering report output on page 154.

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.
Default Font	Set the default font.
Hide # Column	Select to hide the column numbers.
Layout Header	Enter header text and select the header image. Accept the default Fortinet image or click *Browse* to select a different image.
Layout Footer	Select either the default footer or click *Custom* to enter custom footer text in the text field.
Print Cover Page	Select to print the report cover page. Click *Customize* to customize the cover page. See Customizing report cover pages on page 149.

Field	Description
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 dropdown list.
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.
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 dropdown 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*.

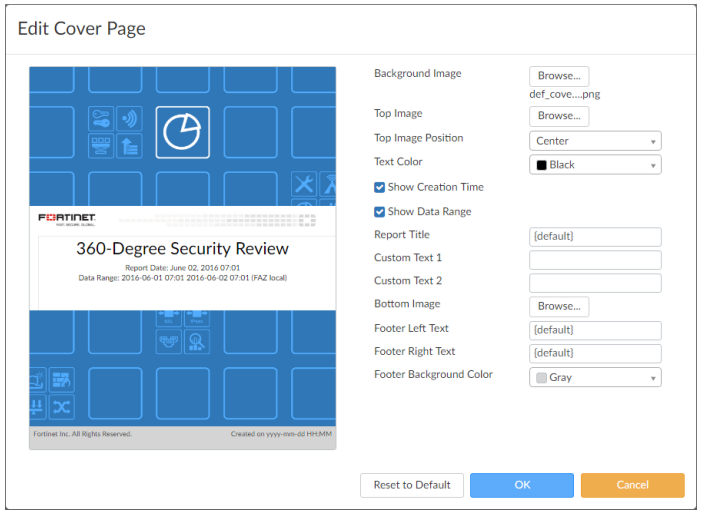
Customizing report cover pages

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

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

To customize a report cover page:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. In the content pane, select the report from the list, and click *Edit* in the toolbar.
4. Select the *Settings* tab and then click *Advanced Settings*.
5. Select the *Print Cover Page* checkbox, then click *Customize* next to the checkbox. The *Edit Cover Page* pane opens.



6. Configure the following settings:

Background Image	Click *Browse* to open the *Choose an Image* dialog box. Select an image or click *Upload File* to find an image on the management computer, then click *OK* to add the image as the background image of the cover page.
Top Image	Click *Browse* to open the *Choose an Image* dialog box. Select an image or click *Upload File* to find an image on the management computer, then click *OK* to add the image at the top of the cover page.
Top Image Position	Select the top image position from the dropdown menu. Select one of the following: *Left*, *Center*, *Right*.
Text Color	Select a text color from the dropdown list.
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	Accept the default title or type another title in the *Report Title* field.
Custom Text 1	If you want, enter custom text for the *Custom Text 1* field.
Custom Text 2	If you want, enter custom text for the *Custom Text 2* field.
Bottom Image	Click *Browse* to open the *Choose an Image* dialog box. Select an image or click *Upload File* to find an image on the management computer, then click *OK* to add the image to the bottom of the cover page.
Footer Left Text	If you want, enter custom text to be printed in the left footer of the cover page.
Footer Right Text	If you want, enter custom text to be printed in the right footer of the cover page.
Footer Background Color	Select the cover page footer background color from the dropdown list.
Reset to Default	Select to reset the cover page settings to their default settings.

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

Reports Layout 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 the layout editor toolbar, or ask you to explicitly agree to it. If you're blocked from accessing the clipboard by clicking the respective cut, copy and paste buttons from the toolbar or context menu, you can always use keyboard shortcuts.

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

Field	Description
Insert Chart or Edit Chart	Click to insert a FortiAnalyzer chart. Charts are associated with datasets that extract data from logs for the report. In the *Insert Chart* or *Chart Properties* dialog box, you can specify a custom title, width, and filters for the chart. For information on setting filters, see Filtering report output on page 154. You can edit a chart by right clicking the chart in the layout editor and selecting *Chart Properties* or by clicking the chart to select it and then clicking *Edit Chart*.
Insert Macro	Click to insert a FortiAnalyzer macro. Macros are associated with datasets that extract data from logs for the report.
Image	Click the *Image* button in the toolbar to insert an image into the report layout. Right-click an existing image to edit image properties.
Table	Click 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	Click to insert a horizontal line.
Insert Page Break for Printing	Click to insert a page break for printing.
Link	Click the *Link* button in the toolbar to open the *Link* dialog box. 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 box.
Anchor	Click the *Anchor* button in the toolbar to insert an anchor in the report layout.
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: • Click the cut button in the toolbar • Right-click and select cut in the menu • 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: • Click the cut button in the toolbar • Right-click and select cut in the menu • Use the *CTRL+C* shortcut on your keyboard.
Paste	To paste text, start with cutting or copying from another source. Depending on the security settings of your browser, you may either paste directly from the clipboard or use the *Paste* dialog box.
Paste as plain text	Click *Paste as plain text* to paste formatted text without the formatting. If the browser blocks the editor toolbar's access to clipboard, a *Paste as Plain Text* dialog box appears and you can paste the fragment into the text box using the *CTRL+V* keyboard shortcut.

Field	Description
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: • Click the *Paste from Word* button in the toolbar • Use the *CTRL+V* shortcut on your keyboard.
Undo	Click to undo the last action. Alternatively, use the *CTRL+Z* keyboard shortcut to perform the undo operation.
Redo	Click to redo the last action. Alternatively, use the *CTRL+Y* keyboard shortcut to perform the redo operation.
Find	Click to find text in the report layout editor. This dialog box includes the following elements: • *Find what*: Is the text field where you enter the word or phrase you want to find. • *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 the search becomes case-sensitive. • *Match whole word*: Checking this option limits the search operation to whole words. • *Match cyclic*: Checking this option means that after the editor reaches the end of the document, the search continues from the beginning of the text. This option is checked by default.
Replace	Click to replace text in the report layout editor. This dialog box includes consists of the following elements: • *Find what*: Is the text field where you enter the word or phrase you want to find. • *Replace with*: Is the text field where you enter the word or phrase that will replace the search term in the document. • *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 the search becomes case-sensitive. • *Match whole word*: Checking this option limits the search operation to whole words. • *Match cyclic*: Checking this option means that after the editor reaches the end of the document, the search continues from the beginning of the text. This option is checked by default.
Save as Template	Click to save the layout as a template.
Paragraph Format	Select the paragraph format from the dropdown list. Select one of the following: *Normal*, *Heading 1*, *Heading 2*, *Heading 3*, *Heading 4*, *Heading 5*, *Heading 6*, *Formatted*, *Address*, or *Normal (DIV)*.
Font Name	Select the font from the dropdown list.

Field	Description
Font Size	Select the font size from the dropdown list. Select a size ranging from 8 to 72.
Bold	Select the text fragment and then click 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 click 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 click 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 click the *Strike Through* button in the toolbar.
Subscript	Select the text fragment and then click the *Subscript* button in the toolbar.
Superscript	Select the text fragment and then click 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, click the *Text Color* button in the toolbar, and select a color.
Background Color	You can also change the color of the text background.
Insert/Remove Numbered List	Click to insert or remove a numbered list.
Insert/Remove Bulleted List	Click to insert or remove a bulleted list.
Decrease Indent	To decrease the indentation of the element, click the *Decrease Indent* toolbar button. The indentation of a block-level element containing the cursor will decrease by one tabulator length.
Increase Indent	To increase the indentation of the element, click 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.

Field	Description
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 to both the left and right margins and the text is not ragged on either side..
Remove Format	Click to remove formatting.

Filtering report output

You can apply log message filters to reports. You can set up report filters in one of the following areas:

- *Settings* tab *Filters* section.
- *Layout* tab *Filters* section in the *Insert Chart* or *Chart Properties* dialog box. To open this dialog box, click *Insert Chart* or *Edit Chart*, or right-click a chart and select *Chart Properties*.

In the *Filters* section, the following options are available.

Field	Description
Log messages that match	Available in the *Settings* tab only. 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	Click to add filters. For each filter, select the field, and operator from the dropdown lists, then enter or select the values as applicable. Filters vary based on device type.
LDAP Query	Available in the *Settings* tab only. Click to add an LDAP query, then select the *LDAP Server* and the *Case Change* value from the dropdown lists. Use this option to query an LDAP server for group membership. The results of this query is used to filter the report to only match logs for users belonging to that group. You must specify the group name in the filter definition. If you enable *LDAP Query*, the group name is not used to match the group field in logs. The group name is only used for the LDAP query to determine group membership.

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	Organizes reports into folders.
Import	Imports a report from a management computer.
Export	Exports a report to a management computer.
Show Scheduled Only	Filters the list to include only reports that have been run or are scheduled to be run.

Organizing reports into folders

You can create folders to organize reports.

To organize reports into folders:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. Click *Folder* in the toolbar, and select *Create New Folder*.
4. Specify the folder name and location and click *OK*. The folder is now displayed in the report list.

You can now create, clone, or import reports into this folder.

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.

Exporting reports only exports the report layout, charts, datasets, and images. Other report configurations are not exported.

To export reports:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.

3. In the content pane, select a report, and select *More* > *Export* in the toolbar to save the file to the management computer.

To import reports:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. In the content pane, click *More* > *Import* in the toolbar. The *Import Report* dialog box opens.
4. Drag and drop the report file onto the dialog box, or click *Browse* and locate the file to be imported on your local computer.
5. Select a folder to save the report to from the dropdown list.
6. Click OK to import the report.

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 the layout editor toolbar, or ask you to explicitly agree to it. If you're blocked from accessing the clipboard by clicking the respective cut, copy and paste buttons from the toolbar or context menu, you can always use keyboard shortcuts.

A report template defines the charts and macros that are 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

Datasets for charts and macros specify what data are used from the Analytics logs when you generate the report. You can also create custom charts and macros for use in report templates.

Creating report templates

You can create a report template by saving a report as a template or by creating a totally new template.

To create a report template:

1. If using ADOMs, ensure you are in the correct ADOM.
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 *Insert Chart* and *Insert Macro* buttons to insert charts and macros into the template.

   For a description of the fields, see Reports Layout tab on page 150. For information about creating charts and macros, see Creating charts on page 160 and Creating macros on page 163.
6. Click *OK*.

   The new template is now displayed on the template list.

To create a report template by saving a report:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *All Reports*.
3. In the content pane, select the report from the list, and click *Edit* in the toolbar.
4. In 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. If using ADOMs, ensure you are in the correct ADOM.
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	Creates a new report template
Edit	Edits 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 cannot delete predefined report templates.
Clone	Clones the selected report template
Rename	Renames the selected report template. You cannot rename predefined report templates.

List of report templates

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

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

FortiGate report templates

Template - 360-Degree Security Review	Template - Security Analysis
Template - Admin and System Events Report	Template - Threat Report
Template - Application Risk and Control	Template - Top 20 Categories and Applications (Session)
Template - Bandwidth and Applications Report	Template - Top 20 Category and Websites (Bandwidth)
Template - Client Reputation	Template - Top 20 Category and Websites (Session)
Template - Cyber Threat Assessment	Template - Top 500 Sessions by Bandwidth
Template - DNS Report	Template - Top Allowed and Blocked with Timestamps
Template - Data Loss Prevention Detailed Report	Template - User Detailed Browsing Log
Template - Detailed Application Usage and Risk	Template - User Security Analysis
Template - Email Report	Template - User Top 500 Websites by Bandwidth
Template - FortiClient Default Report	Template - User Top 500 Websites by Session
Template - FortiClient Vulnerability Scan Report	Template - VPN Report
Template - FortiGate Performance Statistics Report	Template - Web Usage Report
Template - GTP Report	Template - What is New Report
Template - Hourly Website Hits	Template - WiFi Network Summary

Template - IPS Report	Template - Wireless PCI Compliance
Template - PCI-DSS Compliance Review	
Template - SaaS Application Usage Report	

FortiCache report templates

Template - FortiCache Default Report
Template - FortiCache Security Analysis
Template - FortiCache Web Usage Report

FortiClient 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

Chart library

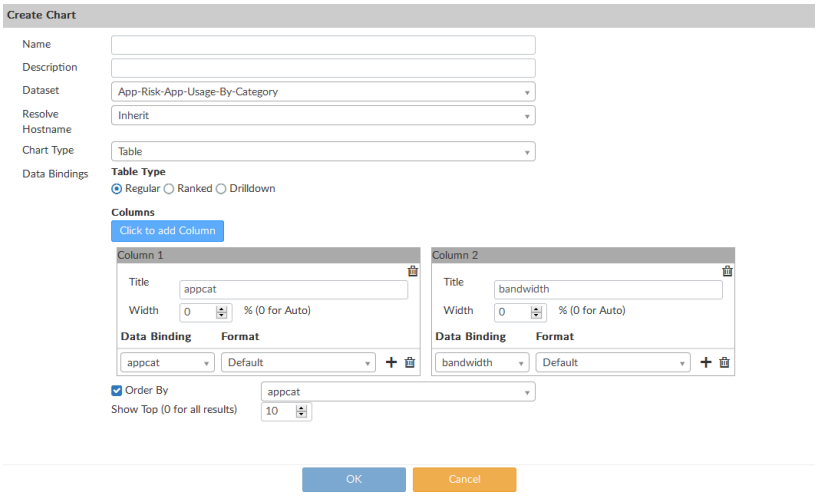
Use the Chart library to create, edit, and manage your charts.

Creating charts

You can also create charts using the *Log View* Chart Builder. See Creating charts on page 120.

To create charts:

1. If using ADOMs, ensure you are in the correct ADOM.
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 dropdown list. For more information, see Datasets on page 165. Options 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 dropdown list; one of: *Table*, *Bar*, *Pie*, *Line*, *Area*, *Donut*, or *Radar*. This selection affects the rest of the available selections.
Data Bindings	The data bindings vary depending on the chart type selected.

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: • *Column Title*: Enter a title for the column. • *Width*: Enter the column width as a percentage. • *Data Binding*: Select a value from the dropdown list. The options vary depending on the selected dataset. • *Format*: Select a value from the dropdown list. • *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.
	Order By	Select what to order the table by. The available options vary depending on the selected dataset.
	Show Top	Enter a numerical value. Only the first 'X' items are 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 are displayed. This options is only available for *Drilldown* tables.
Bar		
	X-Axis	• *Data Binding*: Select a value from the dropdown list. The available options vary depending on the selected dataset. • *Label*: Enter a label for the axis. • *Show Top*: Enter a numerical value. Only the first 'X' items are displayed. Other items are bundled into the *Others* category.
	Y-axis	• *Data Binding*: Select a value from the dropdown list. The available options vary depending on the selected dataset. • *Format*: Select a format from the dropdown list: *Bandwidth*, *Counter*, *Default*, *Percentage*, or *Severity*. • *Label*: Enter a label for the axis.
	Bundle rest into "Others"	Select to bundle the rest of the results into an *Others* category.
	Group By	• *Data Binding*: Select a value from the dropdown list. The available options vary depending on the selected dataset. • *Show Top*: Enter a numerical value. Only the first 'X' items are displayed. Other items can be bundled into the *Others* category.
	Order By	Select to order by the X-Axis or Y-Axis.
Pie, Donut, or Radar		

	Category	• *Data Binding*: Select a value from the dropdown list. The available options vary depending on the selected dataset. • *Label*: Enter a label for the axis. • *Show Top*: Enter a numerical value. Only the first 'X' items are displayed. Other items can be bundled into the *Others* category.
	Series	• *Data Binding*: Select a value from the dropdown list. The available options vary depending on the selected dataset. • *Format*: Select a format from the dropdown list: *Bandwidth*, *Counter*, *Default*, *Percentage*, or *Severity*. • *Label*: Enter a label for the axis.
	Bundle rest into "Others"	Select to bundle the rest of the results into an *Others* category.
Line or Area		
	X-Axis	• *Data Binding*: Select a value from the dropdown list. The available options vary depending on the selected dataset. • *Label*: Enter a label for the axis.
	Lines	• *Data Binding*: Select a value from the dropdown list. The available options vary depending on the selected dataset. • *Format*: Select a format from the dropdown list: *Bandwidth*, *Counter*, *Default*, *Percentage*, or *Severity*. • *Type*: Select the type from the dropdown list: *Line Up* or *Line Down*. • *Legend*: Enter the legend text for the line.
	Add line	Select to add more lines.

5. Click *OK*.

Managing charts

Manage your charts in *Reports* > *Report Definitions* > *Chart 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	Creates a new chart.
Edit	Edits a chart. You can edit charts that you created. You cannot edit predefined 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.

Option	Description
Clone	Clones the selected chart.
Import	Imports a previously exported FortiAnalyzer chart.
Export	Exports one or more FortiAnalyzer charts.
Show Predefined	Displays the predefined charts.
Show Custom	Displays the custom charts.
Search	Lets you search for a chart name.

Viewing datasets associated with charts

To view datasets associated with charts:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports* > *Report Definitions* > *Chart Library*.
3. Select a chart, and click *View* in the toolbar.
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

Use the Macro library to create, edit, and manage your macros.

Creating macros

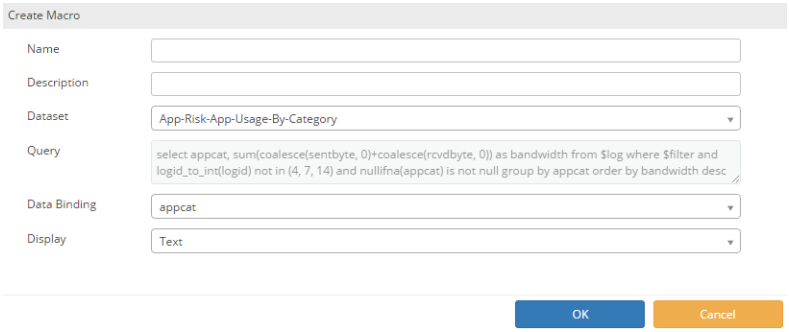
FortiAnalyzer includes a number of predefined macros. You can also create new macros, or clone and edit existing macros.

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. If using ADOMs, ensure you are in the correct ADOM.
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 dropdown 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 dropdown list.
Display	Select a value from the dropdown list.

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

Managing macros

You can manage macros by *Reports* > *Report Definitions* > *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	Creates a new macro.
Edit	Edits 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.

Option	Description
Show Custom	Displays the custom macros.
Search	Lets you search for a macro name.

Viewing datasets associated with macros

To view datasets associated with macros:

1. If using ADOMs, ensure you are in the correct ADOM.
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* or *Edit 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 to view it.

Datasets

Use the Datasets pane to create, edit, and manage your 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. If using ADOMs, ensure you are in the correct ADOM.
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 dropdown list. • 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*, *FortiClient Event*, *FortiClient Traffic*, *FortiClient Vulnerability Scan*, *Web Application Firewall*, *GTP*, *DNS*, and *Local Event*. • The following log types are available for FortiMail: *Email Filter*, *Event*, *History*, and *Virus*. • The following log types are available for FortiWeb: *Intrusion Prevention*, *Event*, and *Traffic*.
Query	Enter the SQL query used for the dataset. An easy way to build a custom query is to copy and modify a predefined dataset's query.
Variables	Click the *Add* button to add variable, expression, and description information.
Test query with specified devices and time period	
Time Period	Use the dropdown list to select a time period. When selecting *Custom*, enter the start date and time, and the 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	Click 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 *Test Result* 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. If using ADOMs, ensure you are in the correct ADOM.
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* field.

SQL query functions

In addition to standard SQL queries, the following are some SQL functions specific to FortiAnalyzer. These are based on standard SQL functions.

`root_domain(hostname)`	The root domain of the FQDN. An example of using this function is: `select devid, root_domain(hostname) as website FROM $log WHERE'user'='USER01' GROUP BY devid, hostname ORDER BY hostname LIMIT 7`
`nullifna(expression)`	This is the inverse operation of `coalesce` that you can use to filter out `n/a` values. This function takes an expression as an argument. The actual SQL syntax this is base on is `select nullif(nullif(expression, 'N/A'), 'n/a')`. In the following example, if the user is n/a, the source IP is returned, otherwise the username is returned. `select coalesce(nullifna('user'), nullifna('srcip')) as user_src, coalesce(nullifna(root_domain(hostname)),'unknown') as domain FROM $log WHERE dstport='80' GROUP BY user_src, domain ORDER BY user_src LIMIT 7`
`email_domain` `email_user`	`email_domain` returns the text after the `@` symbol in an email address. `email_user` returns the text before the `@` symbol in an email address. An example of using this function is: `select 'from' as source, email_user('from') as e_user, email_domain('from') as e_domain FROM $log LIMIT 5 OFFSET 10`
`from_dtime` `from_itime`	`from_dtime(bigint)` returns the device timestamp without time zone. `from_itime(bigint)` returns FortiAnalyzer's timestamp without time zone. An example of using this function is: `select itime, from_itime(itime) as faz_local_time, dtime, from_dtime(dtime) as dev_local_time FROM $log LIMIT 3`

Managing datasets

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

Option	Description
Create New	Creates a new dataset.
Edit	Edits the selected dataset. You can edit datasets that you created. You cannot edit predefined datasets.
View	Displays the settings for the selected dataset. You cannot edit predefined datasets.
Delete	Deletes the selected dataset. You can delete datasets that you create. You cannot delete predefined datasets.

Option	Description
Clone	Clones the selected dataset. You can edit cloned datasets.
Validate	Validate selected datasets.
Validate All Custom	Validates all custom datasets.
Search	Lets you search for a dataset name.

Output profiles

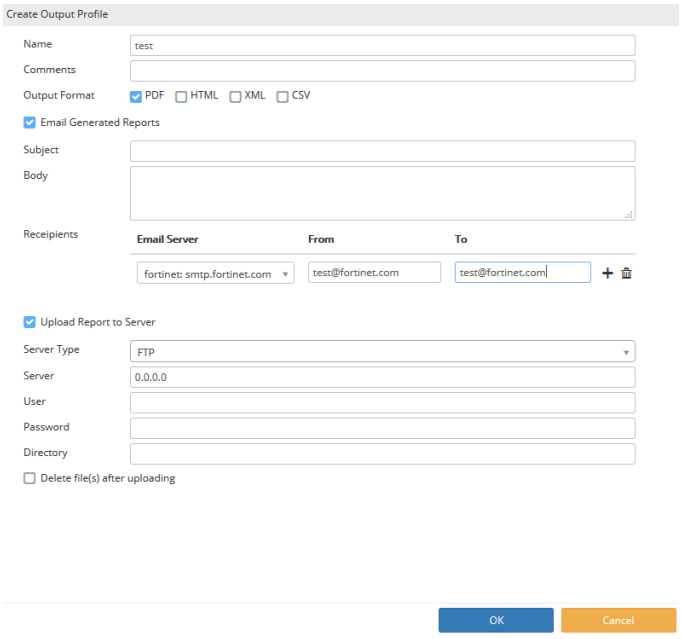
Output profiles allow you to define email addresses to which generated reports are sent and provide an option to upload the reports to FTP, SFTP, or SCP servers. Once created, an output profile can be specified for a report.

Creating output profiles

You must configure a mail server before you can configure an output profile. See Mail Server on page 213.

To create output profiles:

1. If using ADOMs, ensure you are in the correct ADOM.
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 *PDF*, *HTML*, *XML*, or *CSV* format.
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 dropdown list and enter to and from email addresses. Click *Add* 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 dropdown 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	Creates a new output profile.
Edit	Edits the selected output profile.
Delete	Deletes 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. If using ADOMs, ensure you are in the correct ADOM.
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	Creates a new report language placeholder.
View	Views details about the selected report language.
Edit	Edits the selected report language. You cannot edit predefined report languages.
Delete	Deletes the selected report language. You cannot delete predefined report languages.

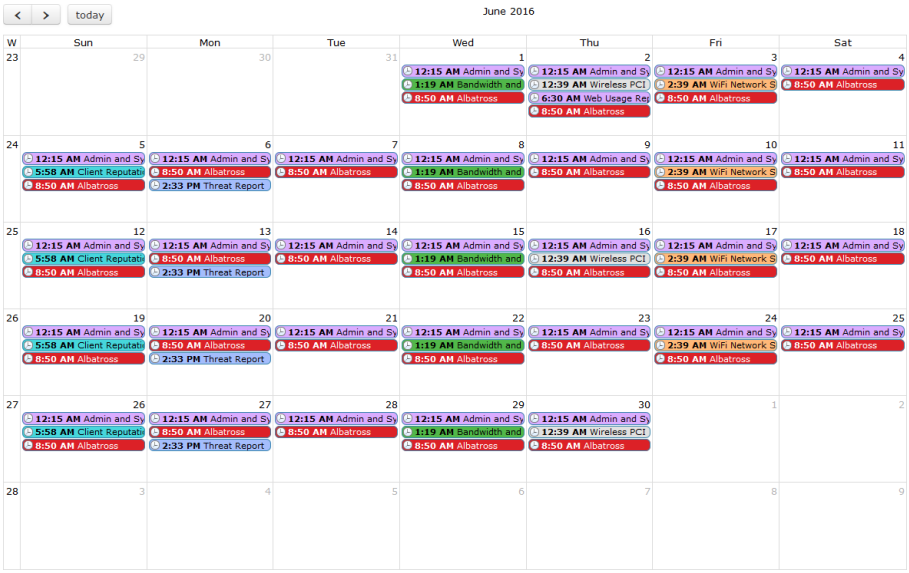
Report calendar

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. If using ADOMs, ensure you are in the correct ADOM.
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.
4. Click a generated report to download it.
5. Click a scheduled report to go to the *Settings* tab of the report.
6. 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.

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

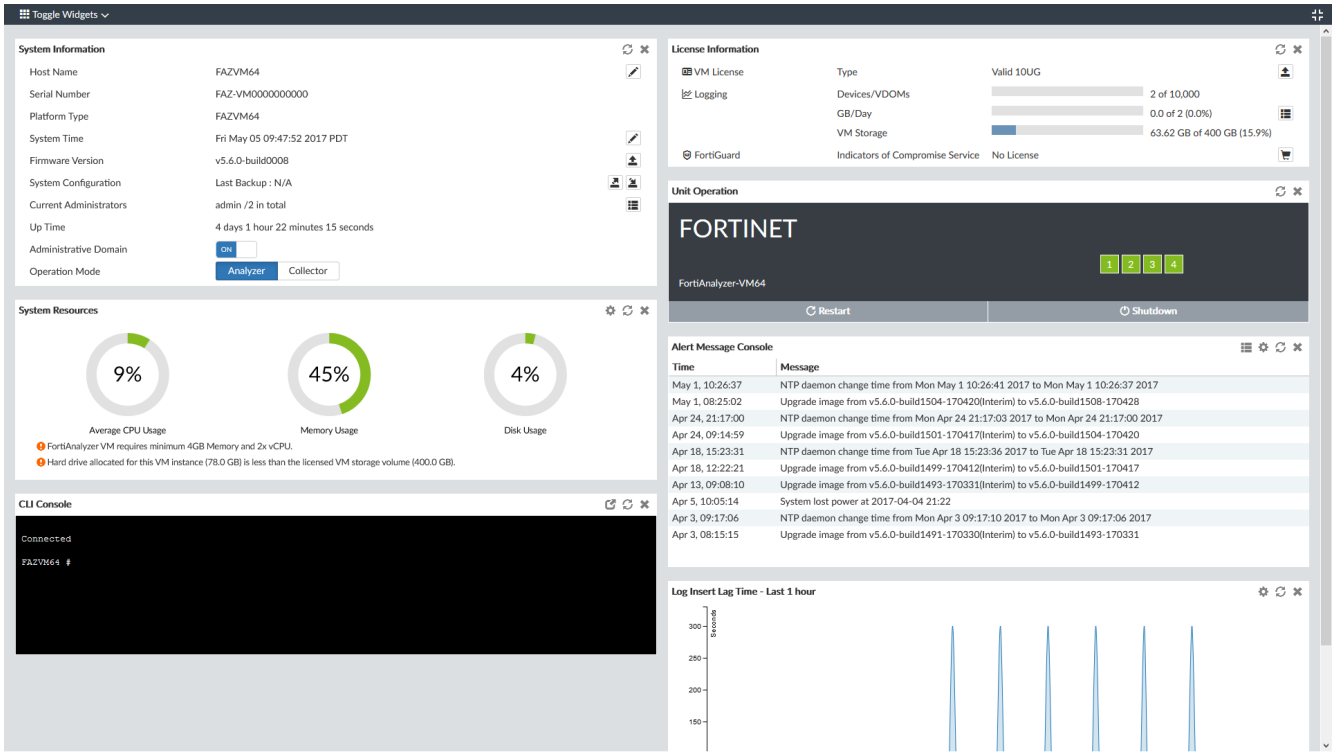
System Settings

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

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.

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.



The following widgets are available:

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. For more information, see System Information widget on page 175. From this widget you can manually update the FortiAnalyzer firmware to a different release. For more information, see Updating the system firmware on page 177. 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 System Resources widget on page 180.
License Information	Displays how many devices of the supported maximum are connected to the FortiAnalyzer unit. See License Information widget on page 180. From this widget you can manually upload a license for 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 Unit Operation widget on page 181.
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 CLI Console widget on page 182.
Alert Message Console	Displays log-based alert messages for both the FortiAnalyzer unit and connected devices. For more information, see Alert Messages Console widget on page 182.
Log Receive Monitor	Displays a real-time monitor of logs received. You can view data per device or per log type. For more information, see Log Receive Monitor widget on page 183.
Insert Rate vs Receive Rate	Displays the log insert and receive rates. For more information, see Insert Rate vs Receive Rate widget on page 183. The *Insert Rate vs Receive Rate* widget is hidden when the FortiAnalyzer is operating in Collector mode, and the SQL database is disabled.
Log Insert Lag Time	Displays how many seconds the database is behind in processing the logs. For more information, see Log Insert Lag Time widget on page 183. The *Log Insert Lag Time* widget is hidden when the FortiAnalyzer is operating in Collector mode, and the SQL database is disabled.
Receive Rate vs Forwarding Rate	Displays the *Receive Rate*, which is the rate at which FortiAnalyzer is receiving logs. For more information, see Receive Rate vs Forwarding Rate widget on page 184.
Disk I/O	Displays the disk utilization, transaction rate, or throughput as a percentage over time. For more information, see Disk I/O widget on page 184.

Customizing the dashboard

The FortiAnalyzer system dashboard can be customized. You can select which widgets to display, where they are located on the page, and whether they are minimized or maximized. It can also be viewed in full screen by selecting the full screen button on the far right side of the toolbar.

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 widget by clicking the Edit icon and configuring the settings.
Reset the dashboard	Select *Toggle Widgets* > *Reset to Default* from the toolbar. The dashboards will be reset to the default view.

System Information widget

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

Host Name	The identifying name assigned to this FortiAnalyzer unit. Click the edit host name button to change the host name. For more information, see Changing the host name on page 176.
Serial Number	The serial number of the FortiAnalyzer unit. The serial number is unique to the FortiAnalyzer unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
Platform Type	Displays the FortiAnalyzer platform type, for example *FAZVM64* (virtual machine).
System Time	The current time on the FortiAnalyzer internal clock. Click the edit system time button to change system time settings. For more information, see Configuring the system time on page 177.
Firmware Version	The version number and build number of the firmware installed on the FortiAnalyzer unit. To update the firmware, you must download the latest version from the Customer Service & Support website at https://support.fortinet.com. Click the update button, then select the firmware image to load from the local hard disk or network volume. For more information, see Updating the system firmware on page 177.

System Configuration	The date of the last system configuration backup. The following actions are available: • Click the backup button to backup the system configuration to a file; see Backing up the system on page 178. • Click the restore to restore the configuration from a backup file; see Restoring the configuration on page 179. You can also migrate the configuration to a different FortiAnalyzer model by using the CLI. See Migrating the configuration on page 179.
Current Administrators	The number of administrators currently logged in. Click the current session list button to view the session details for all currently logged in administrators.
Up Time	The duration of time the FortiAnalyzer unit has been running since it was last started or restarted.
Administrative Domain	Displays whether ADOMs are enabled. Toggle the switch to change the Administrative Domain state. See Enabling and disabling the ADOM feature on page 45.
Operation Mode	Displays the current operation mode of the FortiAnalyzer. Click the other mode to change to it. For more information on operation modes, see Two operation modes on page 17.

Changing the host name

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

- It appears in the *System Information* widget on the dashboard. For more information about the *System Information* widget.
- 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. However, if the host name is longer than 16 characters, the CLI and other places display the host name in a truncated form ending with a tilde (~) to indicate that additional characters exist, but are not displayed. For example, if the host name is FortiAnalyzer1234567890, the CLI prompt would be `FortiAnalyzer123456~#`.

To change the host name:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, click the edit host name button next to the *Host Name* field.
3. In the *Host Name* box, type a new host name.

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

Configuring the system time

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

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

To configure the date and time:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, click the edit system time button next to the *System Time* field.
3. Configure the following settings to either manually configure the system time, or to automatically synchronize the FortiAnalyzer unit's clock with an NTP server:

System Time	The date and time according to the FortiAnalyzer unit's clock at the time that this pane 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: YYYY/MM/DD.
Select Time	Select the time.
Synchronize with NTP Server	Automatically synchronize the date and time.
Sync Interval	Enter how often, in minutes, 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.

4. Click the checkmark to apply your changes.

Updating the system firmware

To take advantage of the latest features and fixes, the FortiAnalyzer firmware can be updated. For information about upgrading your FortiAnalyzer device, see the *FortiAnalyzer Upgrade Guide* or contact Fortinet Customer Service & Support.

Backup the configuration and database before changing the firmware of your FortiAnalyzer unit. Changing the firmware to an older or incompatible version may reset the configuration and database to the default values for that firmware version, resulting in data loss. For information on backing up the configuration, see Backing up the system on page 178.

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

To update the FortiAnalyzer firmware:

1. Download the firmware (the `.out` file) from the Customer Service & Support website, https://support.fortinet.com/.
2. Go to *System Settings* > *Dashboard*.
3. In the *System Information* widget, in the *Firmware Version* field, click *Upgrade Firmware*. The *Firmware Upload* dialog box opens.
4. Drag and drop the file onto the dialog box, or click *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support portal and then click *Open*.
5. Click *OK*. Your device will upload the firmware image and you will receive a confirmation message noting that the upgrade was successful.

Optionally, you can upgrade firmware stored on an FTP or TFTP server using the following CLI command:

```
execute restore image {ftp | tftp} <file path to server> <IP of
     server> <username on server> <password>
```

For more information, see the FortiAnalyzer CLI Reference.

6. Refresh the browser and log back into the device.
7. Launch the *Device Manager* module and make sure that all formerly added devices are still listed.
8. Launch other functional modules and make sure they work properly.

Backing up the system

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

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

To back up the FortiAnalyzer configuration:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, click the backup button next to *System Configuration*. The *Backup System* dialog box opens
3. If you want to encrypt the backup file, select the *Encryption* box, then type and confirm the password you want to use. The password can be a maximum of 63 characters.
4. Select *OK* and save the backup file on your management computer.

Restoring the configuration

You can use the following procedure to restore your FortiAnalyzer configuration from a backup file on your management computer.

To restore the FortiAnalyzer configuration:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, click the restore button next to *System Configuration*. The *Restore System* dialog box opens.
3. Configure the following settings then select *OK*.

Choose Backup File	Select *Browse* to find the configuration backup file you want to restore, or drag and drop the file onto the dialog box.
Password	Type the encryption password, if applicable.
Overwrite current IP and routing settings	Select the checkbox to overwrite the current IP and routing settings.

Migrating the configuration

You can back up the system of one FortiAnalyzer model, and then use the CLI and the FTP, SCP, or SFTP protocol to migrate the settings to another FortiAnalyzer model.

You need the username and password for the FortiAnalyzer model to which you are migrating the configuration file.

If you encrypted the FortiAnalyzer configuration file when you created it, you need the password to decrypt the configuration file when you migrate the file to another FortiAnalyzer model.

To migrate the FortiAnalyzer configuration:

1. In one FortiAnalyzer model, go to *System Settings* > *Dashboard*.
2. Back up the system. See Backing up the system on page 178.
3. In the other FortiAnalyzer model, go to *System Settings* > *Dashboard*.
4. In the *CLI Console* widget, type the following command:

```
execute migrate all-settings <ftp | scp | sftp> <server> <filepath> <user> <password>
      [cryptpasswd]
```

Configuring the operation mode

The FortiAnalyzer unit has two operation modes: Analyzer and Collector. For more information, see Two operation modes on page 17.

When FortiAnalyzer is operating in Collector mode, the SQL database is disabled by default so logs that require the SQL database are not available in Collector mode unless the SQL database is enabled.

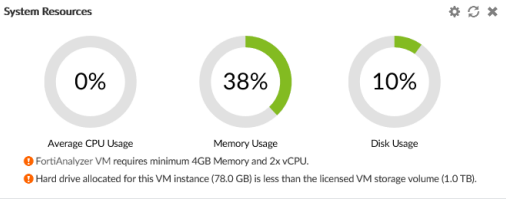
To change the operation mode:

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, select *Analyzer* or *Collector* in the *Operation Mode* field
3. Click *OK* in the confirmation dialog box to change the operation mode.

System Resources widget

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.

On VMs, warning messages are displayed if the amount of memory or the number of CPUs assigned are too low, or if the allocated hard drive space is less than the licensed amount. These warnings are also shown in the notification list (see GUI overview on page 23). Clicking on a warning opens the *FortiAnalyzer VM Install Guide*.

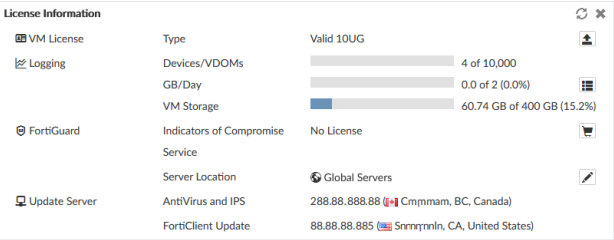


To toggle between real-time and historical data, click *Edit* in the widget toolbar, select *Historical* or *Real-time*, edit the other settings as required, then click *OK*.

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.

License Information widget

The *License Information* widget displays the number of devices connected to the FortiAnalyzer.

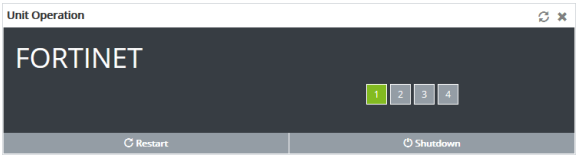


VM License		VM license information and status. Click the upload license button to upload a new VM license file. This field is only visible for FortiAnalyzer VM.
Logging		
	Device/VDOMs	The total number of devices and VDOMs connected to the FortiManager and the total number of device and VDOM licenses.
	GB/Day	The gigabytes per day of logs allowed and used for this FortiAnalyzer. Click the show details button to view the GB per day of logs used for the previous 6 days.
	VM Storage	The amount of VM storage used and remaining. This field is only visible for FortiAnalyzer VM.
FortiGuard		
	Indicators of Compromise Service	The license status. Click the purchase button to go to the Fortinet Customer Service & Support website, where you can purchase a license.
	Secure DNS Server	The SDNS server license status. Click the upload image button to upload a license key.
	Server Location	The locations of the FortiGuard servers, either global or US only. Click the edit icon to adjust the location. Changing the server location will cause the FortiAnalyzer to reboot.
Update Server		
	AntiVirus and IPS	The IP address and physical location of the Antivirus and IPS update server.
	FortiClient Update	The IP address and physical location of the FortiClient update server.

Unit Operation widget

The *Unit Operation* widget graphically displays the status of each port. The port name indicates its status by its color. Green indicates the port is connected. Grey indicates 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.



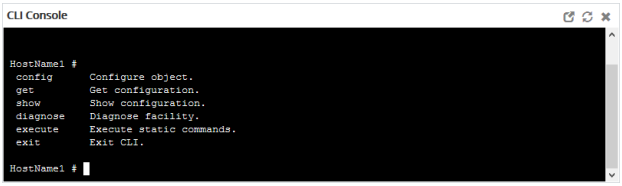
CLI Console widget

The *CLI Console* widget enables you to type command lines through the GUI, without making a separate Telnet, SSH, or local console connection to access the CLI.

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

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

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



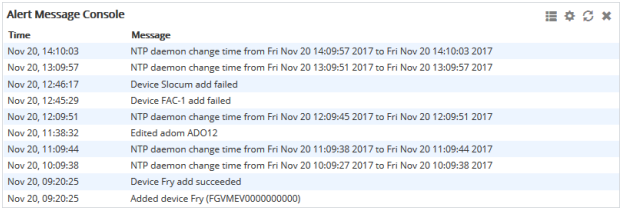
Click *Detach* in the widget toolbar to open the widget in a separate window.

Alert Messages Console widget

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

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

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



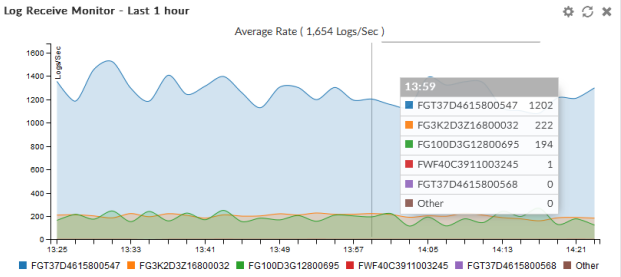
Click *Edit* from the widget toolbar to view the *Alert Message Console Settings*, where you can adjust the number of entries that are visible in the widget, and the refresh interval.

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.

Log Receive Monitor widget

The *Log Receive Monitor* widget displays the rate at which the FortiAnalyzer unit receives logs over time. Log data can be displayed by either log type or device.

Hover the cursor over a point on the graph to see the exact number of logs that were received at a specific time. Click the name of a device or log type to add or remove it from the graph. Click *Edit* in the widget toolbar to modify the widget's settings.



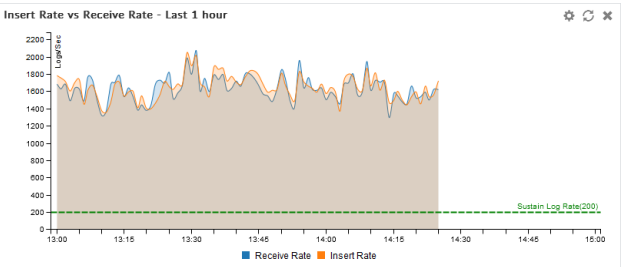
Insert Rate vs Receive Rate widget

The *Insert Rate vs Receive Rate* widget displays the log insert and log receive rates over time.

- Log receive rate: how many logs are being received.
- Log insert rate: how many logs are being actively inserted into the database.

If the log insert rate is higher than the log receive rate, then the database is rebuilding. The lag is the number of logs waiting to be inserted.

Hover the cursor over a point on the graph to see the exact number of logs that were received and inserted at a specific time. Click *Receive Rate* or *Insert Rate* to remove those data from the graph. Click the edit icon in the widget toolbar to adjust the time interval shown on the graph and the refresh interval.

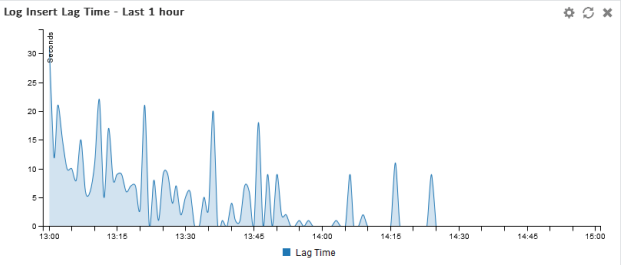


This widget is hidden when FortiAnalyzer is operating in Collector mode, and the SQL database is disabled.

Log Insert Lag Time widget

The *Log Insert Lag Time* widget displays how many seconds the database is behind in processing the logs.

Click the edit icon in the widget toolbar to adjust the time interval shown on the graph and the refresh interval (0 to disable) of the widget.

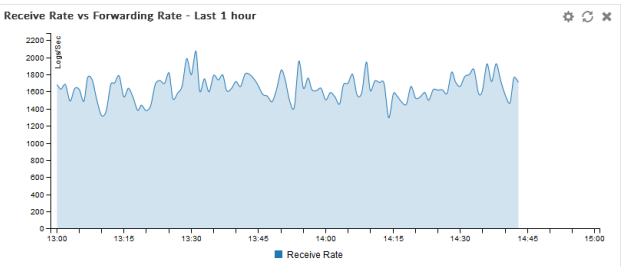


This widget is hidden when FortiAnalyzer is operating in Collector mode, and the SQL database is disabled.

Receive Rate vs Forwarding Rate widget

The *Receive Rate vs Forwarding Rate* widget displays the rate at which the FortiAnalyzer is receiving logs.

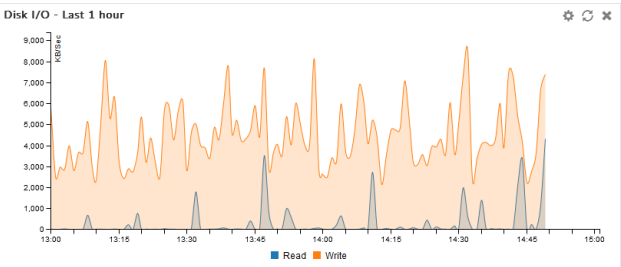
Click the edit icon in the widget toolbar to adjust the time period shown on the graph and the refresh interval, if any, of the widget.



Disk I/O widget

The *Disk I/O* widget shows the disk utilization (%), transaction rate (requests/s), or throughput (KB/s), versus time.

Click the edit icon in the widget toolbar to select which chart is displayed, the time period shown on the graph, and the refresh interval (if any) of the chart.

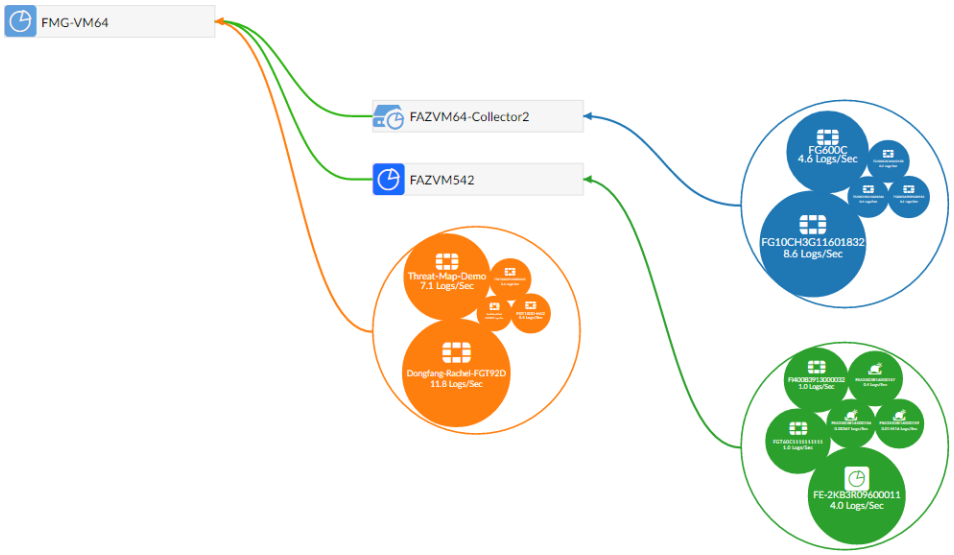


Logging Topology

The *Logging Topology* pane shows the physical topology of devices in the security fabric. Click, hold, and drag to adjust the view in the content pane, and double-click or use the scroll wheel to change the zoom.

The visualization can be filtered to show only FortiAnalyzer devices or all devices by device count or traffic.

Hovering the cursor over a device in the visualization will show information about the device, such as the IP address and device name. Right-click on a device and select *View Related Logs* to go to the *Log View* pane, filtered for that device.



Certificates

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

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

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

The CRL is a list of certificates that have been revoked and are no longer usable. This list includes expired, stolen, or otherwise compromised certificates. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and include 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 versions.

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*.

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

Creating a local certificate

To create a certificate request:

1. Go to *System Settings* > *Certificates* > *Local Certificates*
2. Click *Create New* in the toolbar. The *Generate Certificate Signing Request* pane opens.
3. Enter the following information as required, then click *OK* to save the certificate request:

Certificate Name		The name of the certificate.
Subject Information		Select the ID type from the dropdown list: • *Host IP*: Select if the unit has a static IP address. Enter the public IP address of the unit in the *Host IP* field. • *Domain Name*: Select if the unit has a dynamic IP address and subscribes to a dynamic DNS service. Enter the domain name of the unit in the *Domain Name* field. • Email: Select to use an email address. Enter the email address in the *Email Address* field.
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 (-) icons.
	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 dropdown 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. A name can be: • e-mail address • IP address • URI • DNS name (alternatives to the Common Name) • directory name (alternatives to the Distinguished Name) You must precede the name with the name type. Examples: • IP:1.1.1.1 • email:test@fortinet.com • email:my@other.address • URI:http://my.url.here/
Key Type	The key type can be *RSA* or *Elliptic Curve*.
Key Size	Select the key size from the dropdown list: *512 Bit*, *1024 Bit*, *1536 Bit*, or *2048 Bit*. This option is only available when the key type is *RSA*.
Curve Name	Select the curve name from the dropdown list: *secp256r1* (default), *secp384r1*, or *secp521r1*. This option is only available when the key type is *Elliptic Curve*.
Enrollment Method	The enrollment method is set to *File Based*.

Importing local certificates

To import a local certificate:

1. Go to *System Settings* > *Certificates* > *Local Certificates*.
2. Click *Import* in the toolbar or right-click and select *Import*. The *Import* dialog box opens.
3. Enter the following information as required, then click *OK* to import the local certificate:

Type	Select the certificate type from the dropdown list: *Local Certificate*, *PKCS #12 Certificate*, or *Certificate*.
Certificate File	Click *Browse...* and locate the certificate file on the management computer, or drag and drop the file onto the dialog box.
Key File	Click *Browse...* and locate the key file on the management computer, or drag and drop the file onto the dialog box. This option is only available when *Type* is *Certificate*.
Password	Enter the certificate password. This option is only available when *Type* is *PKCS #12 Certificate* or *Certificate*.

Certificate Name	Enter the certificate name. This option is only available when *Type* is *PKCS #12 Certificate* or *Certificate*.

Deleting local certificates

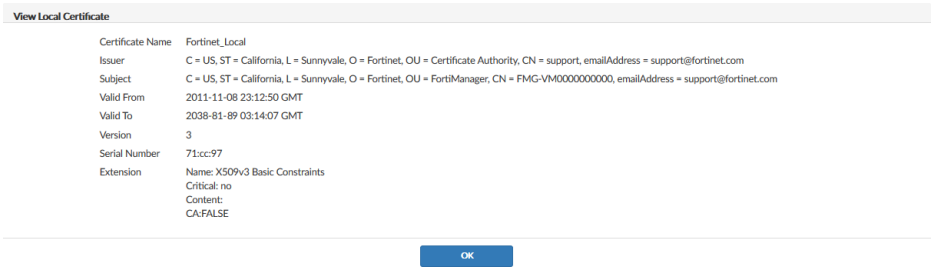
To delete a local certificate or certificates:

1. Go to *System Settings* > *Certificates* > *Local Certificates*.
2. Select the certificate or certificates you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected certificate or certificates.

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 click *View Certificate Detail* in the toolbar or right-click menu. The *View Local Certificate* page opens.



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

Downloading local certificates

To download a local certificate:

1. Go to *System Settings* > *Certificates* > *Local Certificates*.
2. Select the certificate that you need to download.
3. Click *Download* in the toolbar, or right-click and select *Download*, and save the certificate to the management computer.

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. Click *Import* in the toolbar, or right-click and select *Import*. The *Import* dialog box opens.
3. Click *Browse...* and locate the certificate file on the management computer, or drag and drop the file onto the dialog box.
4. Click *OK* to import the certificate.

Viewing CA certificate details

To view a CA certificate's details:

1. Go to *System Settings* > *Certificates* > *CA Certificates*.
2. Select the certificates you need to see details about.
3. Click *View Certificate Detail* in the toolbar, or right-click and select *View Certificate Detail*. The *View CA Certificate* page opens.
4. Click *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 you need to download.
3. Click *Download* in the toolbar, or right-click and select *Download*, 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 you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected certificate or certificates.

The *Fortinet_CA* certificate cannot be deleted.

Certificate revocation lists

When you apply for a signed personal or group certificate to install on remote clients, you can obtain the corresponding root certificate and Certificate Revocation List (CRL) from the issuing CA.

The CRL is a list of certificates that have been revoked and are no longer usable. This list includes expired, stolen, or otherwise compromised certificates. 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. Click *Import* in the toolbar, or right-click and select *Import*. The *Import* dialog box opens.
3. Click *Browse...* and locate the CRL file on the management computer, or drag and drop the file onto the dialog box.
4. Click *OK* to import the CRL.

Viewing a CRL

To view a CRL:

1. Go to *System Settings* > *Certificates* > *CRL*.
2. Select the CRL you need to see details about.
3. Click *View Certificate Detail* in the toolbar, or right-click and select *View Certificate Detail*. The *Result* page opens.
4. Click *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 you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *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 *client* is the FortiAnalyzer unit that forwards logs to another device. The *server* is the FortiAnalyzer unit, syslog server, or CEF server that receives the logs.

In addition to forwarding logs to another unit or server, the client retains a local copy of the logs. The local copy of the logs is subject to the data policy settings for archived logs. See Log storage on page 19 for more information.

To see a graphical view of the log forwarding configuration, and to see details of the devices involved, go to *System Settings* > *Logging Topology*. For more information, see Logging Topology on page 185.

Modes

FortiAnalyzer supports two log forwarding modes: forwarding (default), and aggregation.

Forwarding

Logs are forwarded in real-time or near real-time as they are received. Forwarded content files include: DLP files, antivirus quarantine files, and IPS packet captures.

This mode can be configured in both the GUI and CLI.

Aggregation

As FortiAnalyzer receives logs from devices, it stores them, and then forwards the collected logs at a specified time every day.

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

The client must provide super user log in credentials to get authenticated by the server to aggregate logs.

Aggregation mode can only be configured with the `log-forward` and `log-forward-service` CLI commands. See the *FortiAnalyzer CLI Reference* for more information.

Configuring log forwarding

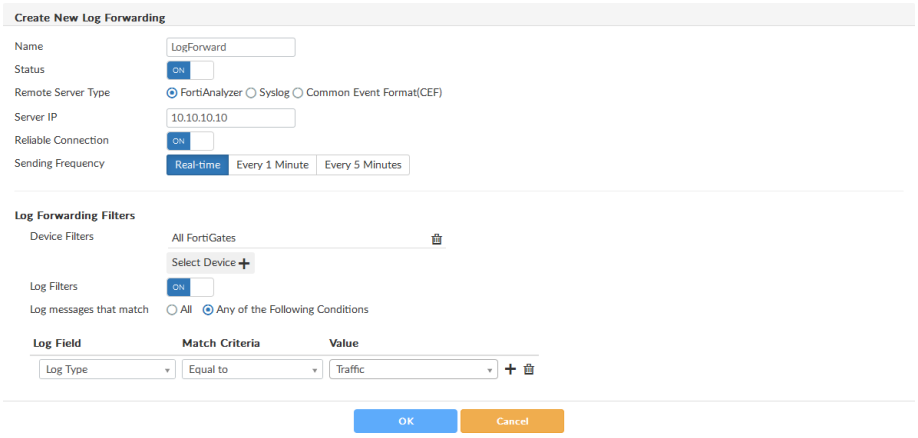
Forwarding mode only requires configuration on the client side. No configuration is needed on the server side. In aggregation mode, accepting the logs must be enabled on the FortiAnalyzer that is acting as the server.

Forwarding mode

Forwarding mode can be configured in the GUI. No configuration is required on the server side.

To configure the client:

1. Go to *System Settings* > *Log Forwarding*.
2. Click *Create New* in the toolbar. The *Create New Log Forwarding* pane opens.



3. Fill in the information as per the below table, then click *OK* to create the new log forwarding. The FortiAnalyzer device will start forwarding logs to the server.

Name	Enter a name for the remote server.
Status	Set to *On* to enable log forwarding. Set to *Off* to disable log forwarding.
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 number. Default: 514. This option is only available when the server type in not *FortiAnalyzer*.
Reliable Connection	Turn on to use TCP connection. Turn off to use UDP connection. If you are forwarding logs to a Syslog or CEF server, ensure this option is supported before turning it on.
Sending Frequency	Select when logs will be sent to the server: *Real-time*, *Every 1 Minute*, or *Every 5 Minutes* (default). This option is only available when the server type is *FortiAnalyzer*.
Log Forwarding Filters	
Device Filters	Click *Select Device*, then select the devices whose logs will be forwarded.

Log Filters	Turn on to configure filter on the logs that are forwarded. Select *All* or *Any of the Following Conditions* in the *Log messages that match* field to control how the filters are applied to the logs. Add filters to the table by selecting the *Log Field*, *Match Criteria*, and *Value* for each filter.
Enable Exclusions	This option is only available when the remove server is a Syslog or CEF server. Turn on to configure filter on the logs that are forwarded. Add exclusions to the table by selecting the *Device Type* and *Log Type*. Then, add *Log Fields* to the *Exclusion List* by clicking *Fields* and specifying the excluded log fields in the *Select Log Field* pane.

Devices whose logs are being forwarded to another FortiAnalyzer device are added to the server as unregistered devices. To register devices, see Adding devices manually on page 80.

Aggregation mode

Aggregation mode can only be configured using the CLI. Aggregation mode configurations are not listed in the GUI table, but still use a log forwarding ID number.

Use the following CLI command to see what log forwarding IDs have been used:

```
get system log-forward
```

To configure the server:

1. If required, create a new administrator with the *Super_User* profile. See Creating administrators on page 55.
2. Enable log aggregation and, if necessary, configure the disk quota, with the following CLI commands:

```
config system log-forward-service
   set accept-aggregation enable
   set aggregation-disk-quota <quota>
end
```

To configure the client:

1. Open the log forwarding command shell:

```
config system log-forward
```

2. Create a new, or edit an existing, log forwarding entry:

```
edit <log forwarding ID>
```

3. Set the log forwarding mode to `aggregation`:

```
set mode aggregation
```

4. Set the server display name and IP address:

```
set server-name <string>
set server-ip <xxx.xxx.xxx.xxx>
```

5. Enter the user name and password of the super user administrator on the server:
```
set agg-user <string>
set agg-password <string>
```
6. If required, set the aggregation time from 0 to 23 hours (default: 0, or midnight):
```
set agg-time <integer>
```
7. Enter the following to apply the configuration and create the log aggregation:
```
end
```
The following line will be displayed to confirm the creation of the log aggregation:
```
check for cfg[<log forwarding ID>] svr_disp_name=<server-name>
```

For more information, see the *FortiAnalyzer CLI Reference*.

Managing log forwarding

Log forwarding mode server entries can be edited and deleted using both the GUI and the CLI. Aggregation mode server entries can only be managed using the CLI. Entries cannot be enabled or disabled using the CLI.

To enable or disable a log forwarding server entry:

1. Go to *System Settings* > *Log Forwarding*.
2. Double-click on a server entry, right-click on a server entry and select *Edit*, or select a server entry then click *Edit* in the toolbar. The *Edit Log Forwarding* pane opens.
3. Set the *Status* to *Off* to disable the log forwarding server entry, or set it to *On* to enable the server entry.
Only the name of the server entry can be edited when it is disabled.
4. Click *OK* to apply your changes.

To edit a log forwarding server entry using the GUI:

1. Go to *System Settings* > *Log Forwarding*.
2. Double-click on a server entry, right-click on a server entry and select *Edit*, or select a server entry then click *Edit* in the toolbar. The *Edit Log Forwarding* pane opens.
3. Edit the settings as required, then click *OK* to apply your changes.

To edit a log forwarding server entry using the CLI:

1. Open the log forwarding command shell:
```
config system log-forward
```
2. Enter an existing entry using its log forwarding ID:
```
edit <log forwarding ID>
```
3. Edit the settings as required. See the *FortiAnalyzer CLI Reference* for information.
4. Enter the following command to apply your changes:
```
end
```

To delete a log forwarding server entry or entries using the GUI:

1. Go to *System Settings* > *Log Forwarding*.
2. Select the entry or entries you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected entry or entries.

To delete a log forwarding server entry using the CLI:

1. Open the log forwarding command shell:
   ```
   config system log-forward
   ```
2. Delete an entry using its log forwarding ID:
   ```
   delete <log forwarding ID>
   ```
   The log forwarding server entry is immediately deleted. There is no confirmation.

To delete all log forwarding entries using the CLI:

1. Enter the following CLI command:
   ```
   config system log-forward
      purge
   ```
2. Enter `y` to delete all the entries.
   ```
   This operation will clear all table!
   Do you want to continue? (y/n)y
   ```

Fetcher Management

Log fetching is used to retrieve archived logs from one FortiAnalyzer device to another. This allows administrators to run queries and reports against historic data, which can be useful for forensic analysis.

The fetching FortiAnalyzer can query the server FortiAnalyzer and retrieve the log data for a specified device and time period, based on specified filters. The retrieved data are then indexed, and can be used for data analysis and reports.

Log fetching can only be done on two FortiAnalyzer devices running the same firmware. A FortiAnalyzer device can be either the fetch server or the fetching client, and it can perform both roles at the same time with different FortiAnalyzer devices. Only one log fetching session can be established at a time between two FortiAnalyzer devices.

The basic steps for fetching logs are:

1. On the client, create a fetching profile. See Fetching profiles on page 196.
2. On the client, send the fetch request to the server. See Fetch requests on page 197.
3. If this is the first time fetching logs with the selected profile, or if any changes have been made to the devices and/or ADOMs since the last fetch, on the client, sync devices and ADOMs with the server. See Synchronizing devices and ADOMs on page 198.
4. On the server, review the request, then either approve or reject it. See Request processing on page 198.
5. Monitor the fetch process on either FortiAnalyzer. See Fetch monitoring on page 199.
6. On the client, wait until the database is rebuilt before using the fetched data for analysis.

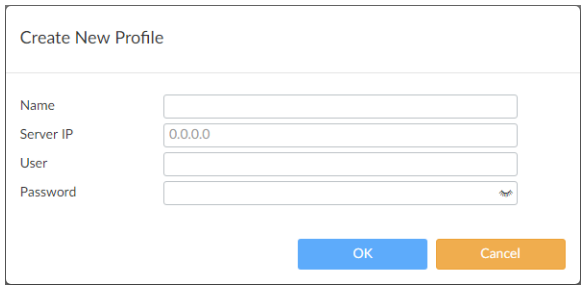
Fetching profiles

Fetching profiles can be managed from the *Profiles* tab on the *System Settings* > *Fetcher Management* pane.

Profiles can be created, edited, and deleted as required. The profile list shows the name of the profile, as well as the IP address of the server it fetches from, the server and local ADOMs, and the administrator name on the fetch server.

To create a new fetching profile:

1. On the client, go to *System Settings* > *Fetcher Management*.
2. Select the *Profiles* tab, then click *Create New* in the toolbar, or right-click and select *Create New* from the menu. The *Create New Profile* dialog box opens.



3. Configure the following settings, then click *OK* to create the profile.

Name	Enter a name for the profile.
Server IP	Enter the IP address of the fetch server.
User	Enter the username of an administrator on the fetch server, which, together with the password, authenticates the fetch client's access to the fetch server.
Password	Enter the administrator's password, which, together with the username, authenticates the fetch client's access to the fetch server.

The fetch server administrator user name and password must be for an administrator with either a *Standard_User* or *Super_User* profile.

To edit a fetching profile:

1. Go to *System Settings* > *Fetching Management*.
2. Double-click on a profile, right-click on a profile then select *Edit*, or select a profile then click *Edit* in the toolbar. The *Edit Profile* pane opens.
3. Edit the settings as required, then click *OK* to apply your changes.

To delete a fetching profile or profiles:

1. Go to *System Settings* > *Fetching Management*.
2. Select the profile or profiles you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected profile or profiles.

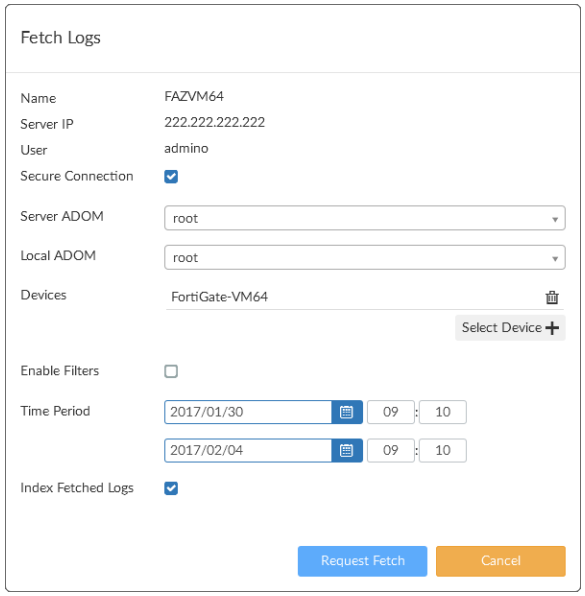
Fetch requests

A fetch request requests archived logs from the fetch server configured in the selected fetch profile. When making the request, the ADOM on the fetch server the logs are fetched from must be specified. An ADOM on the fetching client must be specified or, if needed, a new one can be created. If logs are being fetched to an existing local ADOM, you must ensure the ADOM has enough disk space for the incoming logs.

The data policy for the local ADOM on the client must also support fetching logs from the specified time period. It must keep both archive and analytics logs long enough so they will not be deleted in accordance with the policy. For example: Today is July 1, the ADOM's data policy is configured to keep analytics logs for 30 days (June 1 - 30), and you need to fetch logs from the first week of May. The data policy of the ADOM must be adjusted to keep analytics and archive logs for at least 62 days to cover the entire time span. Otherwise, the fetched logs will be automatically deleted after they are fetched.

To send a fetch request:

1. On the fetch client, go to *System Settings* > *Fetcher Management* and select the *Profiles* tab
2. Select the profile then click *Request Fetch* in the toolbar, or right-click and select *Request Fetch* from the menu. The *Fetch Logs* dialog box opens.



3. Configure the following settings, then click *Request Fetch*.

The request is sent to the fetch server. The status of the request can be viewed in the *Sessions* tab.

Name	Displays the name of the fetch server you have specified.
Server IP	Displays the IP address of the server you have specified.
User	Displays the username of the server administrator you have provided.
Secure Connection	Select to use SSL connection to transfer fetched logs from the server.
Server ADOM	Select the ADOM on the server the logs will be fetched from. Only one ADOM can be fetched from at a time.

Local ADOM	Select the ADOM on the client where the logs will be received. Either select an existing ADOM from the dropdown list, or create a new ADOM by entering a name for it into the field.
Devices	Add the devices the logs will be fetched from. Up to 256 devices can be added. Click *Select Device*, select devices from the list, then click *OK*.
Enable Filters	Select to enable filters on the logs that will be fetched. Select *All* or *Any of the Following Conditions* in the *Log messages that match* field to control how the filters are applied to the logs. Add filters to the table by selecting the *Log Field*, *Match Criteria*, and *Value* for each filter.
Time Period	Specify what date and time range of log messages to fetch.
Index Fetch Logs	If selected, the fetched logs will be indexed in the SQL database of the client once they are received. Select this option unless you want to manually index the fetched logs.

Synchronizing devices and ADOMs

If this is the first time the fetching client is fetching logs from the device, or if any changes have been made the devices or ADOMs since the last fetch, then the devices and ADOMs must be synchronized with the server.

To synchronize devices and ADOMs:

1. On the client, go to *System Settings* > *Fetcher Management* and select the *Profiles* tab
2. Select the profile then click *Sync Devices* in the toolbar, or right-click and select *Sync Devices* from the menu. The *Sync Server ADOM(s) & Device(s)* dialog box opens and shows the progress of the process.

   Once the synchronization is complete, you can verify the changes on the client. For example, newly added devices in the ADOM specified by the profile.

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 as required.

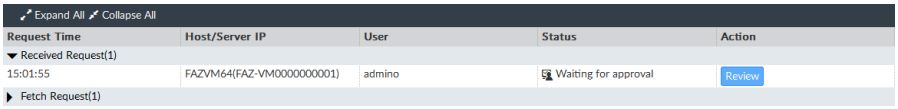
Request processing

After a fetching client has made a fetch request, the request will be listed on the fetch server in the *Received Request* section of the *Sessions* tab on the *Fetcher Management* pane. It will also be available from the notification center in the GUI banner.

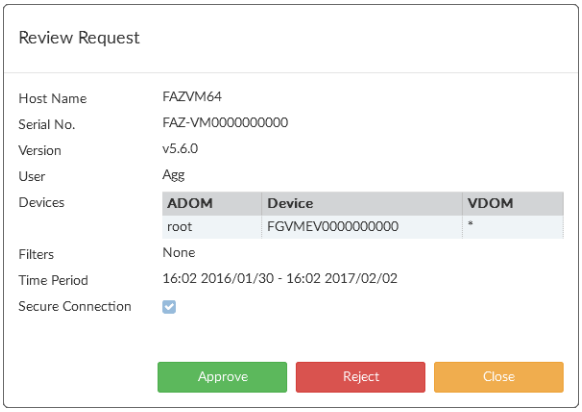
Fetch requests can be approved or rejected.

To process the fetch request:

1. Go to the notification center in the GUI banner and click the log fetcher request, or go to the *Sessions* tab on the *System Settings* > *Fetcher Management* pane.



2. Find the request in the *Received Request* section. You may have to expand the section, or select *Expand All* in the content pane toolbar. The status of the request will be *Waiting for approval*.
3. Click *Review* to review the request. The *Review Request* dialog box will open.



4. Click *Approve* to approve the request, or click *Reject* to reject the request.

   If you approve the request, the server will start to retrieve the requested logs in the background and send them to the client. If you reject the request, the request will be canceled and the request status will be listed as *Rejected* on both the client and the server.

Fetch monitoring

The progress of an approved fetch request can be monitored on both the fetching client and the fetch server.

Go to *System Settings* > *Fetcher Management* and select the *Sessions* tab to monitor the fetch progress. A fetch session can be paused by clicking *Pause*, and resumed by clicking *Resume*. It can also be canceled by clicking *Cancel*.

Once the log fetching is completed, the status changes to *Done* and the request record can be deleted by clicking *Delete*. The client will start to index the logs into the database.

It can take a long time for the client to finish indexing the fetched logs and make the analyzed data available. A progress bar is shown in the GUI banner; for more information, click on it to open the *Rebuild Log Database* dialog box.

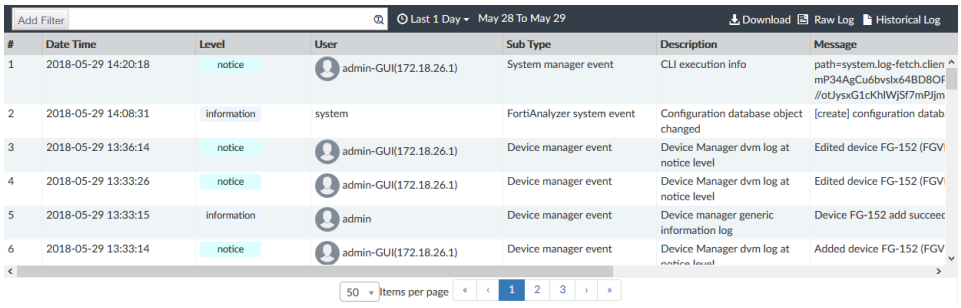
Log and report features will not be fully available until the rebuilding process is complete.

Event Log

The *Event Log* pane provides an audit log of actions made by users on FortiAnalyzer. It allows you to view log messages that are stored in memory or on the internal hard disk drive. You can use filters to search the messages and download the messages to the management computer.

See the *FortiAnalyzer Log Message Reference*, available from the Fortinet Document Library, for more information about the log messages.

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



The following options are available:

Add Filter	Filter the event log list based on the log level, user, sub type, or message. See Event log filtering on page 202.
Download	Download the event logs in either CSV or the normal format to the management computer.
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.
Back	Click the back icon to return to the regular view from the historical view.
View	View the selected log file. This option is also available from the right-click menu, or by double-clicking on the log file. This option is only available when viewing historical event logs.
Delete	Delete the selected log file. This option is also available from the right-click menu. This option is only available when viewing historical event logs.
Clear	Clear the selected file of logs. This option is also available from the right-click menu. This option is only available when viewing historical event logs.

Type	Select the type from the dropdown list: • *Event Log* • *FDS Upload Log*: Select the device from the dropdown list. • *FDS Download Log*: Select the service (*FDS*, or *FCT*) from the *Service* dropdown list, select the event type (*All Event*, *Push Update*, *Poll Update*, or *Manual Update*) from the *Event* dropdown list, and then click *Go* to browse the logs. This option is only available when viewing historical logs.
Search	Enter a search term to search the historical logs. This option is only available when viewing historical event logs.
Pagination	Browse the pages of logs and adjust the number of logs that are shown per page.

The following information is shown:

#	The log number.
Date Time	The date and time that the log file was generated.
Level	The log level: Debug, Error, Information, Critical, Notification, Alert, Warning, Emergency
User	The user that the log message relates to.

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

Event log filtering

The event log can be filtered using the *Add Filter* box in the toolbar.

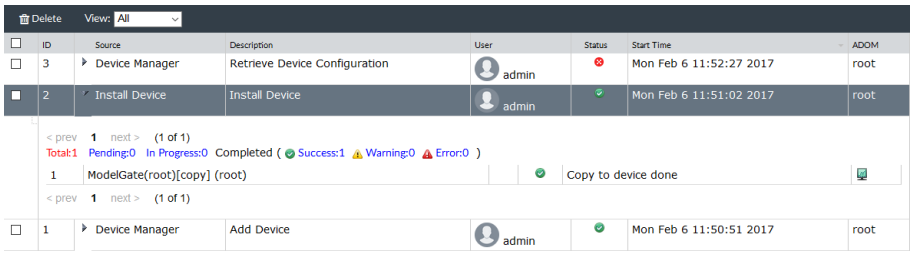
To filter FortiView summaries using the toolbar:

1. Specify filters in the *Add Filter* box.
   - Regular Search: In the selected summary view, click in the *Add Filter* box, select a filter from the dropdown list, then type a value. Click NOT to negate the filter value. You can add multiple filters at a time, and connect them with an "or".
   - Advanced Search: Click the *Switch to Advanced Search* icon at the right end of the *Add Filter* box to switch to advanced search mode. In this mode, you type in the whole search criteria (log field names and values). Click the *Switch to Regular Search* icon to return to regular search.
2. Click *Go* to apply the filter.

Task Monitor

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

Go to *System Settings* > *Task Monitor* to view the task monitor. The task list size can also be configured; see



The following options are available:

Delete	Remove the selected task or tasks from the list. This changes to *Cancel Running Task(s)* when *View* is *Running*.
View	Select which tasks to view from the dropdown list, based on their status. The available options are: *Running*, *Pending*, *Done*, *Error*, *Cancelling*, *Cancelled*, *Aborting*, *Aborted*, *Warning*, and *All*.
Expand Arrow	In the *Source* column, select the expand arrow icon to display the specific actions taken under this task. To filter the specific actions taken for a task, select one of the options on top of the action list. Select the history icon to view specific information on task progress. This can be useful when troubleshooting warnings and errors.
Group Error Devices	Select *Group Error Devices* to create a group of the failed devices, allowing for re-installations to easily be done on only the failed devices.
History	Click the history icon to view task details in a new window.
Pagination	Browse the pages of tasks and adjust the number of tasks shown per page.

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): • *Done*: Completed with success. • *Error*: Completed without success. • *Canceled*: User canceled the task. • *Canceling*: User is canceling the task. • *Aborted*: The FortiAnalyzer system stopped performing this task. • *Aborting*: The FortiAnalyzer system is stopping performing this task. • *Running*: Being processed. In this status, a percentage bar appears in the Status column. • *Pending* • *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.

SNMP

Enable the SNMP agent on the FortiAnalyzer device so it can send traps to and receive queries from the computer that is designated as its SNMP manager. This allows for monitoring the FortiAnalyzer with an SNMP manager.

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

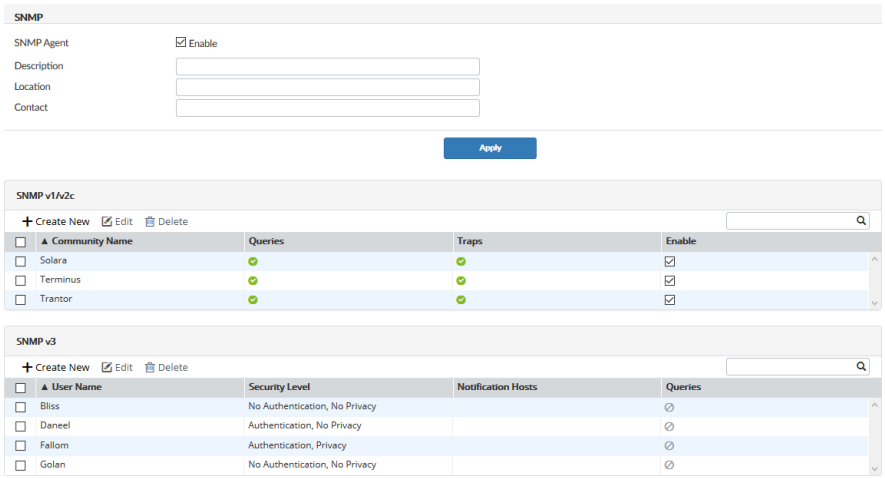
The FortiAnalyzer SNMP implementation is read-only — SNMP v1, v2c, and v3 compliant SNMP manager applications, such as those on your local computer, have read-only access to FortiAnalyzer system information and can receive FortiAnalyzer system traps.

SNMP agent

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

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

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



The following information and options are available:

SNMP Agent	Select to enable the SNMP agent. When this is enabled, it sends FortiAnalyzer SNMP traps.
Description	Optionally, type a description of this FortiAnalyzer system to help uniquely identify this unit.
Location	Optionally, type the location of this FortiAnalyzer system to help find it in the event it requires attention.
Contact	Optionally, type the contact information for the person in charge of this FortiAnalyzer system.
SNMP v1/2c	The list of SNMP v1/v2c communities added to the FortiAnalyzer configuration.
Create New	Select *Create New* to add a new SNMP community. If SNMP agent is not selected, this control will not be visible. For more information, see SNMP v1/v2c communities on page 206.
Edit	Edit the selected SNMP community.
Delete	Delete the selected SNMP community or communities.
Community Name	The name of the SNMP community.
Queries	The status of SNMP queries for each SNMP community. The enabled icon indicates that at least one query is enabled. The disabled icon indicates that all queries are disabled.
Traps	The status of SNMP traps for each SNMP community. The enabled icon indicates that at least one trap is enabled. The disabled icon indicates that all traps are disabled.
Enable	Enable or disable the SNMP community.
SNMP v3	The list of SNMPv3 users added to the configuration.

Create New	Select *Create New* to add a new SNMP user. If SNMP agent is not selected, this control will not be visible. For more information, see SNMP v3 users on page 209.
Edit	Edit the selected SNMP user.
Delete	Delete the selected SNMP user or users.
User Name	The user name for the SNMPv3 user.
Security Level	The security level assigned to the SNMPv3 user.
Notification Hosts	The notification host or hosts assigned to the SNMPv3 user.
Queries	The status of SNMP queries for each SNMP user. The enabled icon indicates queries are enabled. The disabled icon indicates they are disabled.

SNMP v1/v2c communities

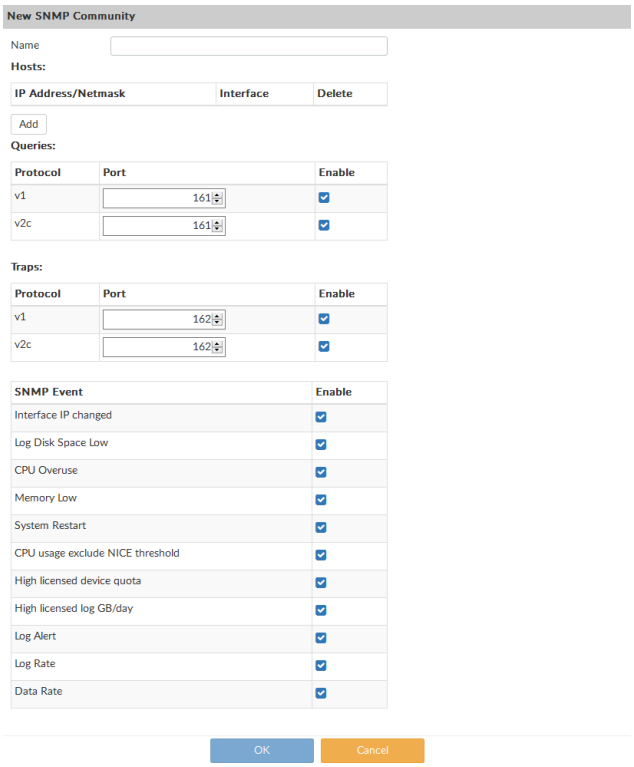
An SNMP community is a grouping of equipment for network administration purposes. You must configure your FortiAnalyzer to belong to at least one SNMP community so that community's SNMP managers can query the FortiAnalyzer system information and receive SNMP traps from it.

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 create a new SNMP community:

1. Go to *System Settings* > *Advanced* > *SNMP* and ensure the SNMP agent is enabled.
2. In the *SNMP v1/v2c* section, click *Create New* in the toolbar. The *New SNMP Community* pane opens.



3. Configure the following options, then click *OK* to create the community.

Name		Enter a name to identify the SNMP community. This name cannot be edited later.
Hosts		The list of hosts that can use the settings in this SNMP community to monitor the FortiAnalyzer system. When you create a new SNMP community, there are no host entries. Select *Add* to create a new entry that broadcasts the SNMP traps and information to the network connected to the specified interface.
	IP Address/Netmask	Enter the IP address and netmask 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 interface that connects to the network where this SNMP manager is located from the dropdown list. This must be done if the SNMP manager is on the Internet or behind a router.
	Delete	Click the delete icon to remove this SNMP manager entry.
	Add	Select to add another entry to the Hosts list. Up to eight SNMP manager entries can be added for a single community.

Queries	Enter the port number (161 by default) 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	Enter the Remote port number (162 by default) 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 SNMP traps to be sent to the community. • *Interface IP changed* • *Log disk space low* • *CPU Overuse* • *Memory Low* • *System Restart* • *CPU usage exclude NICE threshold* • *RAID Event* (only available for devices that support RAID) • *Power Supply Failed* (only available on supported hardware devices) • *High licensed device quota* • *High licensed log GB/day* • *Log Alert* • *Log Rate* • *Data Rate* FortiAnalyzer feature set SNMP events:

To edit an SNMP community:

1. Go to *System Settings* > *Advanced* > *SNMP*.
2. In the *SNMP v1/v2c* section, double-click on a community, right-click on a community then select *Edit*, or select a community then click *Edit* in the toolbar. The *Edit SNMP Community* pane opens.
3. Edit the settings as required, then click *OK* to apply your changes.

To delete an SNMP community or communities:

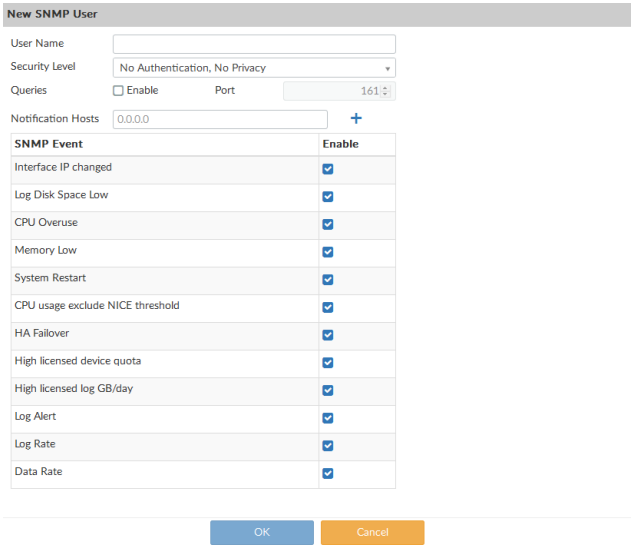
1. Go to *System Settings* > *Advanced* > *SNMP*.
2. In the *SNMP v1/v2c* section, select the community or communities you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected community or communities.

SNMP v3 users

The FortiAnalyzer SNMP v3 implementation includes support for queries, traps, authentication, and privacy. SNMP v3 users can be created, edited, and deleted as required.

To create a new SNMP user:

1. Go to *System Settings* > *Advanced* > *SNMP* and ensure the SNMP agent is enabled.
2. In the *SNMP v3* section, click *Create New* in the toolbar. The *New SNMP User* pane opens.



3. Configure the following options, then click *OK* to create the community.

User Name	The name of the SNMP v3 user.
Security Level	The security level of the user. Select one of the following: • *No Authentication, No Privacy* • *Authentication, No Privacy*: Select the *Authentication Algorithm* (SHA1, MD5) and enter the password. • *Authentication, Privacy*: Select the *Authentication Algorithm* (SHA1, MD5), the *Private Algorithm* (AES, DES), and enter the passwords.
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 SNMP traps to be sent to the SNMP manager. • *Interface IP changed* • *Log disk space low* • *CPU Overuse* • *Memory Low* • *System Restart* • *CPU usage exclude NICE threshold* • *RAID Event* (only available for devices that support RAID) • *Power Supply Failed* (only available on supported hardware devices) • *High licensed device quota* • *High licensed log GB/day* • *Log Alert* • *Log Rate* • *Data Rate* FortiAnalyzer feature set SNMP events:

To edit an SNMP user:

1. Go to *System Settings* > *Advanced* > *SNMP*.
2. In the *SNMP v3* section, double-click on a user, right-click on a user then select *Edit*, or select a user then click *Edit* in the toolbar. The *Edit SNMP User* pane opens.
3. Edit the settings as required, then click *OK* to apply your changes.

To delete an SNMP user or users:

1. Go to *System Settings* > *Advanced* > *SNMP*.
2. In the *SNMP v3* section, select the user or users you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected user or users.

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.

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

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

SNMP traps

Fortinet devices share SNMP traps, but each type of device also has traps specific to that device type. 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 that is included with the trap, as well as the SNMP MIB field name to help locate the information about the trap.

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:
	`config system snmp sysinfo`
	`  set trap-high-cpu-threshold <percentage value>`
	`end`

Trap message	Description

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:
	`config system snmp sysinfo`
	`set trap-cpu-high-exclude-nice-threshold <percentage value>`
	`end`

Memory low (fnTrapMemThreshold)	Memory usage exceeds 90 percent. This threshold can be set in the CLI using the following commands:
	`config system snmp sysinfo`
	`set trap-low-memory-threshold <percentage value>`
	`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.
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. Available on some devices that 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.
Log rate too high (fmTrapLogRateThreshold)	The incoming log rate has exceeded the peak log rate threshold. To determine the peak log rate, use the following CLI command: `get system loglimits`
Data rate too high (fmTrapLogDataRateThreshold)	The incoming data rate has exceeded the peak data rate threshold. The peak data rate is calculated using the peak log rate x 512 bytes (average log size).

Fortinet & FortiAnalyzer MIB fields

The Fortinet MIB contains fields reporting current Fortinet unit status information. The below tables 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 Server

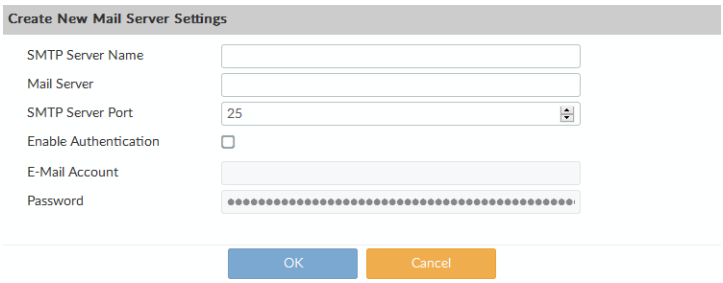
A mail server allows the FortiAnalyzer to sent email messages, such as notifications when reports are run or specific events occur. Mail servers can be added, edited, deleted, and tested.

Go to System *Settings* > *Advanced* > *Mail Server* to configure SMTP mail server settings.

If an existing mail server is in use, the delete icon is removed and the mail server entry cannot be deleted.

To add a mail server:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Click *Create New* in the toolbar. The *Create New Mail Server Settings* pane opens.



3. Configure the following settings and then select *OK* to create the mail server.

SMTP Server Name	Enter a name for the SMTP server.
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. This option is only accessible when authentication is enabled.
Password	Enter the email account password. This option is only accessible when authentication is enabled.

To edit a mail server:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Double-click on a server, right-click on a server and then select *Edit* from the menu, or select a server then click *Edit* in the toolbar. The *Edit Mail Server Settings* pane opens.
3. Edit the settings as required, and then click *OK* to apply the changes.

To test the mail server:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Select the server you need to test.
3. Click *Test* from the toolbar, or right-click and select *Test*.
4. Type the email address you would like to send a test email to and click *OK*. A confirmation or failure message will be displayed.
5. Click *OK* to close the confirmation dialog box.

To delete a mail server or servers:

1. Go to *System Settings* > *Advanced* > *Mail Server*.
2. Select the server or servers you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation box to delete the server.

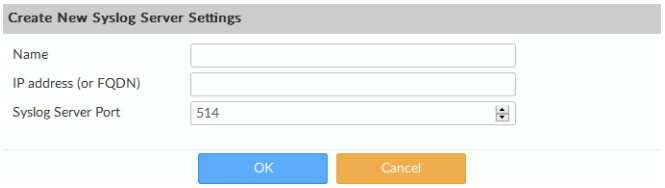
Syslog Server

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

If an existing syslog server is in use, the delete icon is removed and the server entry cannot be deleted.

To add a syslog server:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Click *Create New* in the toolbar. The *Create New Syslog Server Settings* pane opens.



3. Configure the following settings and then select *OK* to create the mail server.

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

To edit a syslog server:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Double-click on a server, right-click on a server and then select *Edit* from the menu, or select a server then click *Edit* in the toolbar. The *Edit Syslog Server Settings* pane opens.
3. Edit the settings as required, and then click *OK* to apply the changes.

To test the syslog server:

1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Select the server you need to test.
3. Click *Test* from the toolbar, or right-click and select *Test*.
   A confirmation or failure message will be displayed.

To delete a syslog server or servers:

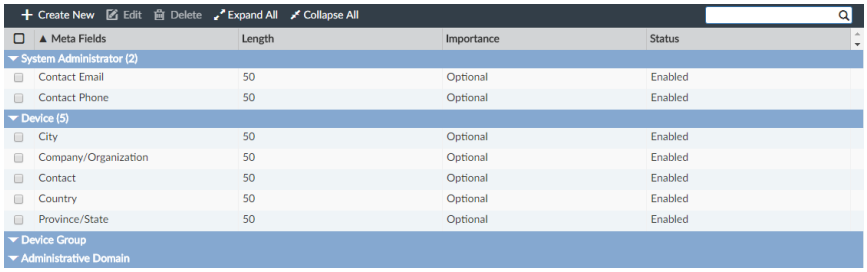
1. Go to *System Settings* > *Advanced* > *Syslog Server*.
2. Select the server or servers you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation box to delete the server or servers.

Meta Fields

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

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

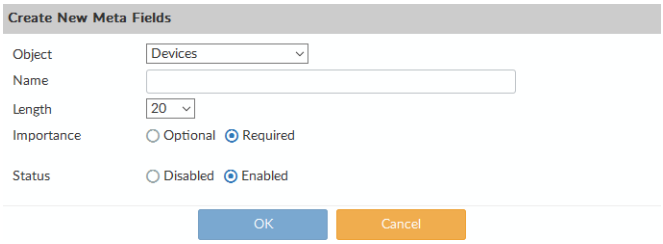
Go to *System Settings* > *Advanced* > *Meta Fields* to configure meta fields. Meta fields can be added, edited, and deleted.



Select *Expand All* or *Contract All* from the toolbar or right-click menu to view all of or none of the meta fields under each object.

To create a new meta field:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Click *Create New* in the toolbar. The *Create New Meta Field* pane opens.



3. Configure the following settings and then select *OK* to create the meta field.

Object	The object this metadata field applies to: *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 dropdown 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*.

To edit a meta field:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Double-click on a field, right-click on a field and then select *Edit* from the menu, or select a field then click *Edit* in the toolbar. The *Edit Meta Fields* pane opens.
3. Edit the settings as required, and then click *OK* to apply the changes.

The *Object* and *Name* fields cannot be edited.

To delete a meta field or fields:

1. Go to *System Settings* > *Advanced* > *Meta Fields*.
2. Select the field or fields you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation box to delete the field or fields.

The default meta fields cannot be deleted.

Device logs

The FortiAnalyzer allows you to log system events to disk. You can control device log file size and the 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.

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:

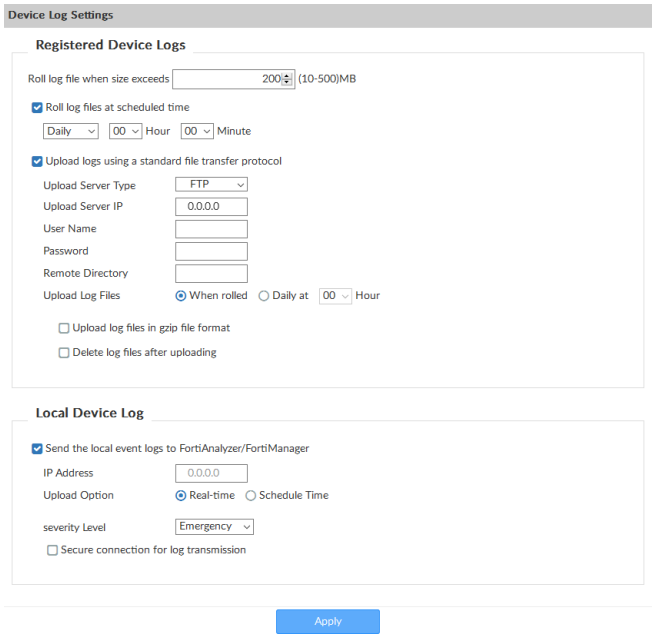
```
FG3K6A3406600001-tlog.1252929496.log-2017-09-29-08-03-54.gz
```

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 using the GUI or CLI.

Configuring rolling and uploading of logs using the GUI

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



Configure the following settings, and then select *Apply*:

Registered Device Logs	
Roll log file when size exceeds	Enter the log file size, from 10 to 500MB. Default: 200MB.
Roll log files at scheduled time	Select to roll logs daily or weekly. • *Daily*: select the hour and minute value in the dropdown lists. • *Weekly*: select the day, hour, and minute value in the dropdown 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	Enter the username used to connect to the upload server.
Password	Enter the password used to connect to the upload server.
Remote Directory	Enter the remote directory on the upload server where the log will be uploaded.
Upload Log Files	Select to upload log files when they are rolled according to settings selected under *Roll Logs*, or daily at a specific hour.

Upload rolled files in gzip file format	Select to gzip the logs before uploading. This will result in smaller logs and faster upload times.
Delete files after uploading	Select to remove device log files from the FortiAnalyzer system after they have been uploaded to the Upload Server.
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 in real time or at a scheduled time. When selecting a scheduled time, you can specify the hour and minute to upload logs each day.
Severity Level	Select the minimum log severity level from the dropdown list. This option is only available when *Upload Option* is *Realtime*.
Secure connection for log transmission	Select to use a secure connection for log transmission.

Configuring rolling and uploading of logs using the CLI

Log rolling and uploading can be enabled and configured using the CLI. For more information, see the *FortiAnalyzer CLI Reference*.

Enable or disable log file uploads

Use the following CLI commands to enable or disable log file uploads.

To enable log uploads:

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

To disable log uploads:

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

Roll logs when they reach a specific size

Use the following CLI commands to specify the size, in MB, at which a log file is rolled.

To roll logs when they reach a specific size:

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

Roll logs on a schedule

Use the following CLI commands to configure rolling logs on a set schedule, or never.

To disable log rolling:

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

To enable daily log rolling:

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

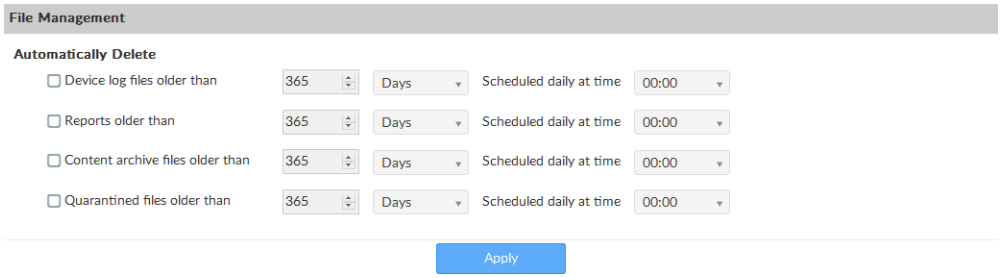
To enable weekly log rolling:

```
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
```

File Management

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

Go to *System Settings* > *Advanced* > *File Management* to configure file management settings.



Configure the following settings, and then select *Apply*:

Device log files older than	Select to enable automatic deletion of compressed log files. Enter a value in the text field, select the time period (*Days*, *Weeks*, or *Months*), and choose a time of day.
Reports older than	Select to enable automatic deletion of reports of data from compressed log files. Enter a value in the text field, select the time period, and choose a time of day.
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, select the time period, and choose a time of day.
Quarantined files older than	Select to enable automatic deletion of compressed log files of quarantined files. Enter a value in the text field, select the time period, and choose a time of day.

The time period you select determines how often the item is checked. If you select *Months*, then the item is checked once per month. If you select *Weeks*, then the item is checked once per week, and so on. For example, if you specify *Device log files older than 3 Months*, then on July 1, the logs for April, May, and June are kept and the logs for March and older are deleted.

Advanced Settings

Go to *System Settings* > *Advanced* > *Advanced Settings* to view and configure advanced settings and download WSDL files.

Configure the following settings and then select *Apply*:

ADOM Mode	Select the ADOM mode, either *Normal* or *Advanced*. Advanced mode will allow you to assign a VDOM from a single device to a different ADOM, but will result in more complicated management scenarios. It is recommended only for advanced users.

Download WSDL file	Select the required WSDL functions then click the *Download* button to download the WSDL file to your management computer. When selecting *Legacy Operations*, no other options can be selected. Web services is a standards-based, platform independent, access method for other hardware and software APIs. The file itself defines the format of commands the FortiAnalyzer will accept as well as the responses 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 administrator can from the GUI or CLI.
Task List Size	Set a limit on the size of the task list. Default: 2000.

FortiManager

When FortiManager features are enabled for the FortiAnalyzer unit, the following panes are available:

Device Manager (for FortiManager)	Add, configure, and manage FortiGate devices.
Policy and Object	Centrally manage FortiGate devices by creating policies and objects and installing them to managed devices.
AP Manager	Centrally manage FortiAP access points by authorizing and monitoring FortiAP devices. You can also edit and monitor authorized devices.
FortiClient Manager	Centrally manage FortiClient profiles for FortiGate devices as well as monitor FortiClient endpoints.
VPN Manager	Centrally manage IPsec VPN communities and SSL-VPN settings.
FortiSwitch Manager	Centrally manage FortiSwitch templates and VLANs, and monitor FortiSwitch devices that are connected to FortiGate devices.

On the System Settings pane, the *HA* pane is also available to configure high availability.

For information about using FortiManager features, see the *FortiManager Administration Guide* or the FortiManager Online Help.

Enable or disable FortiManager features

You can enable FortiManager features on FortiAnalyzer so 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 or disable FortiManager features using either the GUI or CLI.

To enable FortiManager features on FortiAnalyzer from the 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 the 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)
   ```
2. Type `Y`.
3. After the system reboots, log in to the FortiAnalyzer GUI. FortiManager features, except FortiGuard, have been enabled.

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, provide the license key that you have purchased.

To disable FortiManager features on FortiAnalyzer from the 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 no longer includes FortiManager feature tiles.

To disable FortiManager features on FortiAnalyzer using the CLI:

1. 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)
   ```
2. Type `Y`.

Appendix A - Port Numbers

The following tables describe the port numbers that FortiAnalyzer uses:

- ports for traffic originating from units (outbound ports)
- ports for traffic receivable by units (listening ports)
- ports used to connect to the FortiGuard Distribution Network (FDN)

Traffic varies by enabled options and configured ports. Only default ports are listed.

Functionality	Port(s)
DNS lookup	UDP 53
FDN connection	TCP 443
NTP synchronization	UDP 123
SNMP traps	UDP 162
Syslog, log forwarding	UDP 514 If a secure connection is configured between FortiGate and FortiAnalyzer, syslog traffic is sent into an IPsec tunnel. Data is 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 Remote access to quarantine, logs, and reports from FortiGate Remote management from FortiManager (configuration retrieval) (OFTP)	TCP 514
EMS for Chromebooks logging	TCP 8443

FortiAnalyzer listening ports

Functionality	Port(s)
SNMP query	UDP 161
Syslog, log forwarding	UDP 514 If a secure connection is configured between FortiGate and FortiAnalyzer, syslog traffic is sent into an IPsec tunnel. Data is 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 FortiManager	TCP 443
Device registration of FortiGate or FortiManager Receive log file uploading from FortiClient Remote access to quarantine, logs, and reports from FortiGate Remote management from FortiManager (configuration retrieval) (OFTP)	TCP 514
Interface access by FortiManager	TCP 541
HTTP or HTTPS administrative access to the GUI's CLI dashboard widget–using the same protocol used by the administrator when logging in to the GUI.	TCP 2032
Log aggregation server (requires model FortiAnalyzer 800 series or higher).	TCP 3000
Web Service	TCP 8080
Ping	ICMP protocol