



FortiAnalyzer
Version 3.0 MR7

FORTINET™

www.fortinet.com

FortiAnalyzer Administration Guide
Version 3.0 MR7
08 September 2008
05-30007-0082-20080908

© Copyright 2008 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet®, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Regulatory compliance

FCC Class A Part 15 CSA/CUS



CAUTION: Risk of Explosion if Battery is replaced by an Incorrect Type. Dispose of Used Batteries According to the Instructions.

Contents

Introduction	9
About this document.....	9
Fortinet documentation.....	10
Fortinet Tools and Documentation CD	10
Fortinet Knowledge Center	11
Comments on Fortinet technical documentation.....	11
Customer service and technical support	11
What's new for 3.0 MR7	13
3.0 MR7 new features and changes	15
Power supply monitoring for FortiAnalyzer-2000A and 4000A	15
Registered devices' hard limits	15
CLI displays the tasks in the upload queue.....	15
Dashboard enhancements	15
Custom fields for log messages	16
Reports.....	16
Report configuration enhancements.....	16
VoIP reports.....	17
Alert email configuration changes	17
Administrative Domains (ADOMs).....	19
About administrative domains (ADOMs).....	19
Configuring ADOMs	22
Accessing ADOMs as the admin administrator.....	23
Assigning administrators to an ADOM.....	24
System	25
Dashboard	25
Tabs	27
RAID Monitor.....	28
System Information	29
Setting the time.....	29
Changing the host name.....	30
Changing the firmware.....	30
License Information.....	30
System Resources	31
Viewing operational history.....	32
System Operation	33
Formatting the log disks.....	33
Resetting to the default configuration	33
Alert Message Console	34
Viewing alert console messages	34
Statistics.....	35

Viewing session information	35
Filtering session information	36
Report Engine	36
Log Receive Monitor	37
Intrusion Activity	38
Virus Activity	39
Top FTP Traffic	40
Top Email Traffic	41
Top IM/P2P Traffic	42
Top Traffic	43
Top Web Traffic	44
Network	45
Interface	45
Changing interface settings	45
About Fortinet Discovery Protocol	47
DNS	47
Routing	47
Adding a route	48
Admin	48
Adding or editing an administrator account	49
Changing an administrator's password	50
Access Profile	50
Auth Group	51
RADIUS Server	51
Administrator Settings	52
Monitor	52
Network Sharing	53
Adding share users	53
Adding share groups	54
Configuring Windows shares	54
Assigning user permissions	55
Configuring NFS shares	55
Default file permissions on NFS shares	56
Config	56
Automatic file deletion and local log settings	57
Configuring log aggregation	58
Configuring an aggregation client	59
Configuring an aggregation server	59
Configuring log forwarding	60
Configuring IP aliases	60
Importing an IP alias list file	61
IP alias ranges	62
Configuring RAID	62
RAID levels	62
Hot swapping hard disks	64

Hot swapping the FortiAnalyzer-2000/2000A and FortiAnalyzer-4000/4000A	66
Configuring RAID on the FortiAnalyzer-400 and FortiAnalyzer-800/800B.	67
Configuring RAID on the FortiAnalyzer-2000/2000A and FortiAnalyzer-4000/4000A	67
Configuring LDAP connections	68
Maintenance	69
Backup & Restore	69
FortiGuard Center	70
Device	73
Viewing the device list	73
Maximum number of devices	76
Unregistered vs. registered devices	77
Configuring unregistered device connection attempt handling	79
Manually adding a device	80
Classifying FortiGate network interfaces.....	84
Manually adding a FortiGate unit using the Fortinet Discovery Protocol (FDP)	85
Blocking device connection attempts	86
Configuring device groups	88
Log	91
Viewing log messages	91
Viewing current log messages	91
Viewing historical log messages	92
Browsing log files	93
Viewing log file contents.....	94
Importing a log file.....	95
Downloading a log file	96
Customizing the log view	97
Displaying and arranging log columns	97
Filtering logs.....	98
Filtering tips	99
Searching the logs	100
Search tips	102
Printing the search results.....	103
Downloading the search results	103
Rolling and uploading logs	104
Content Archive	107
Viewing content archives	107

Customizing the content archive view	108
Displaying and arranging log columns	109
Filtering logs.....	110
Filtering tips	110
Searching full email content archives	111
Reports	113
Configuring reports.....	113
Configuring report layout.....	114
Editing charts in a report layout	116
Configuring report schedules	118
Configuring data filter templates	121
Configuring report output templates.....	123
Configuring language.....	126
Browsing reports.....	130
Quarantine	131
Viewing quarantined files	131
Alert.....	133
Alert Events.....	133
Adding an alert event	133
Output.....	135
Configuring alerts by email server	135
Testing the mail server configuration.....	136
Configuring SNMP traps and alerts	136
Adding an SNMP server	137
FortiAnalyzer SNMP support.....	138
Configuring alerts by Syslog server	140
Adding a Syslog server.....	140
Network Analyzer.....	141
Connecting the FortiAnalyzer unit to analyze network traffic.....	141
Viewing Network Analyzer log messages	142
Viewing current Network Analyzer log messages.....	143
Viewing historical Network Analyzer log messages.....	143
Browsing Network Analyzer log files	144
Viewing Network Analyzer log file contents	145
Downloading a Network Analyzer log file.....	147
Customizing the Network Analyzer log view	148
Displaying and arranging log columns	148
Filtering logs.....	149
Filtering tips	150

Searching the Network Analyzer logs	150
Search tips	152
Printing the search results.....	153
Downloading the search results	153
Rolling and uploading Network Analyzer logs	153
Tools.....	157
Preparing for the vulnerability scan job.....	157
Preparing Windows target hosts	158
Preparing Unix target hosts.....	160
Viewing vulnerability scan modules	161
Configuring vulnerability scan jobs.....	162
Viewing vulnerability scan reports	166
File Explorer	167
Managing firmware versions.....	169
Backing up your configuration.....	169
Backing up your configuration using the web-based manager	170
Backing up your configuration using the CLI.....	170
Backing up your log files	170
Testing firmware before upgrading	172
Upgrading your FortiAnalyzer unit	174
Upgrading to FortiAnalyzer 3.0	174
Upgrading using the web-based manager.....	174
Upgrading using the CLI	175
Verifying the upgrade	176
Reverting to a previous firmware version	177
Downgrading to FortiLog 1.6.....	177
Verifying the downgrade	178
Downgrading to FortiLog 1.6 using the CLI.....	178
Restoring your configuration	180
Restoring configuration settings on a FortiAnalyzer unit.....	180
Restoring your configuration settings using the web-based manager	182
Restoring your configuration settings using the CLI.....	182

Appendix: FortiAnalyzer reports in 3.0 MR7	185
FortiGate reports	185
Intrusion Activity	186
Antivirus Activity	186
Webfilter Activity	189
Antispam Activity	190
IM Activity	191
VoIP reports	192
Content Activity	193
Network Activity	194
Web Activity	195
Mail Activity	196
FTP Activity	196
Terminal Activity	197
VPN Activity	197
Event Activity	198
P2P Activity	199
Audit Activity	200
Summary Reports	201
Forensic Reports	202
Audit	202
Detailed	202
Summary	203
FortiMail Reports	203
Mail High Level	203
Mail Sender	205
Mail Recipient Activity	206
Mail Destination IP	206
Spam Sender	207
Spam Recipient	208
Spam Destination IP	209
Virus Sender	209
Virus Recipient	211
Virus Destination IP	212
FortiClient Reports	212
Index	213

Introduction

FortiAnalyzer units are network appliances that provide integrated log collection and reporting tools. Reports analyze logs for email, FTP, web browsing, security events, and other network activity to help identify security issues and reduce network misuse and abuse.

In addition to logging and reporting, FortiAnalyzer units also have several major features that augment or enable certain FortiGate unit functionalities, such as content archiving and quarantining, and improve your ability to stay informed about the state of your network.

This chapter contains the following topics:

- [About this document](#)
- [Fortinet documentation](#)
- [Customer service and technical support](#)

About this document

This document describes how to configure and use FortiAnalyzer units through their web-based manager.



Note: The recommended minimum screen resolution for the management computer connecting to the web-based manager is 1280 by 1024 pixels.

This document contains the following chapters:

- [What's new for 3.0 MR7](#) describes what the new maintenance release contains.
- [Administrative Domains \(ADOMs\)](#) describes how to enable and configure domain-based access to data and configurations for connected devices and the FortiAnalyzer unit itself.
- [System](#) describes how to configure FortiAnalyzer system settings, such as network interfaces, system time, administrators, network shares (NAS), and local logging.
- [Device](#) describes how to configure and manage connections to the FortiAnalyzer unit from FortiGate, FortiMail, FortiClient, FortiManager, and Syslog device types.
- [Log](#) describes how to view logs from devices or the FortiAnalyzer unit itself. It also describes how to customize the log view.
- [Content Archive](#) describes how to view logs and files that have been full and/or summary content archived by FortiGate units using the FortiGate content archiving feature.
- [Quarantine](#) describes how to view files quarantined by FortiGate units, and to configure the quarantine disk space quota.

- [Reports](#) describes how to configure report profiles for one-time or scheduled reports on your network devices, users, or groups.
- [Alert](#) describes how to define log message criteria that signify critical network events. As log messages arrive, if they meet those criteria, FortiAnalyzer units send alert messages using a method of your choice: email, SNMP, or Syslog. This chapter also lists SNMP traps that the FortiAnalyzer unit supports.
- [Network Analyzer](#) describes how to connect the FortiAnalyzer unit to a span or mirror port on a network switch to analyze, or sniff, the network traffic passing through the FortiAnalyzer unit.
- [Tools](#) describes how to configure vulnerability scans and view the resulting reports as well as viewing all files on the FortiAnalyzer unit.
- [Managing firmware versions](#) describes how to properly back up your current configuration, upgrade/downgrade firmware, and restore your configuration. This chapter also describes how to test a firmware image before installing the image on the FortiAnalyzer unit.
- [Appendix: FortiAnalyzer reports in 3.0 MR7](#) describes the FortiAnalyzer reports that changed or were moved to other categories or both. This appendix also includes what reports were removed and what were unchanged in FortiAnalyzer 3.0 MR7.

Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

The following [FortiAnalyzer product documentation](#) is available:

- *FortiAnalyzer Administration Guide*
Describes how to use the web-based manager of the FortiAnalyzer unit to configure all available features.
- *FortiAnalyzer CLI Reference*
Describes how to use the command line interface of the FortiAnalyzer unit to configure all available features, CLI structure and available commands.
- *FortiAnalyzer online help*
Provides a searchable version of the *Administration Guide* in HTML format. You can access context-appropriate online help using the online help button in the web-based manager as you work.
- *FortiAnalyzer QuickStart Guides*
Describes how to install and set up the FortiAnalyzer unit.
- *FortiAnalyzer Install Guide*
Describes in detail how to install and set up the FortiAnalyzer unit, how to connect to the CLI and web-based manager, default settings, and how to manage firmware.

Fortinet Tools and Documentation CD

All Fortinet documentation is available from the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation, see the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

Fortinet Knowledge Center

The knowledge center contains short how-to articles, FAQs, technical notes, product and feature guides, and much more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Visit the Fortinet Technical Support web site at <http://support.fortinet.com> to learn about the technical support services that Fortinet provides.

What's new for 3.0 MR7

This section lists and describes the new features and changes in FortiAnalyzer 3.0 MR7. The chapter, [“Managing firmware versions” on page 169](#), provides detailed information about how to properly upgrade to FortiAnalyzer 3.0 MR7.

New CLI commands, as well as changes to existing CLI commands, are found in the What's new chapter of the *FortiAnalyzer CLI Reference*.

The following bulleted list includes links to other sections in this document where you can find additional information about these new features and changes.

New features and changes for FortiAnalyzer 3.0 MR7 are:

- **High-end FortiAnalyzer units support additional terabytes (TB) of space** – The higher-end FortiAnalyzer units, such as the FortiAnalyzer-2000/2000A and FortiAnalyzer-4000/4000A, now support up to 8 TB for log disk file systems. There is no additional information available.
- **Power supply monitoring feature** – A new feature, power supply monitoring, provides a notification when a power supply failure occurs or an administrator adds a power supply to the FortiAnalyzer unit. See [“Power supply monitoring for FortiAnalyzer-2000A and 4000A” on page 15](#) for more information.
- **Registered devices' limits changed** – Registered device limits have increased. See [“Maximum number of devices” on page 76](#) for more information.
- **Web-based manager change** – The Action column is now an unnamed column across all menus and tabs within the web-based manager. There is no additional information on this change.
- **CLI displays tasks in the upload queue** – The command, `diagnose upload status`, displays what files are waiting to be uploaded. See [“CLI displays the tasks in the upload queue” on page 15](#) for more information.
- **Dashboard enhancements** – There are several new widgets added to the Dashboard in FortiAnalyzer, including a widget for configuring and displaying RAID status. See [“Dashboard” on page 25](#) for more information.
- **Administration admin name enhancement** – Administrators can now configure names with the @ symbol. For additional information, see [“Admin” on page 48](#) in the System chapter.
- **HTTPS certificates** – Administrators can now change and customize (text only) HTTPS certificates. This is only available in the CLI. See the *FortiAnalyzer CLI Reference* for additional information.
- **Security engine removed** – The security engine feature has been removed for FortiAnalyzer 3.0 MR7. There is no additional information available.
- **Software RAID changes** – When using software RAID5, the system becomes overloaded on units with software RAID. If redundancy is required, Fortinet now recommends RAID 10. RAID 5, unless selected from the CLI, will not appear on the web-based manager. For additional information, see [“Configuring RAID” on page 62](#) in the System chapter.

- **Network Summary menu removed** – The Network Summary menu was removed in FortiAnalyzer 3.0 MR7. This menu was removed because most of the information that previously displayed, now displays as widgets on the Dashboard. See [“Dashboard” on page 25](#) for more information about these new widgets that have replaced the Network Summary menu.
- **Log Viewer menu enhancements** – When viewing real-time logs or historical logs, the options Resolve Host and Resolve Service are no longer available. From within the Real-time tab, you can now view up to 1000 log messages; you can also view up to 1000 log messages from the Historical tab as well. See [“Viewing log messages” on page 91](#) for more information.
- **Custom fields for log messages** – You can now enable custom fields for log messages that are received from FortiGate units from the CLI. See [“Custom fields for log messages” on page 16](#) for more information.
- **Report configuration enhancements** – Reports contain several enhancements in FortiAnalyzer 3.0 MR7, as well as the additional of VoIP reports. See both [“Report configuration enhancements” on page 16](#) and [“Reports” on page 113](#) for more information.
- **Logs for HA members** – Logs that are viewed on the FortiGate unit now contain device ID fields for HA members. See the *FortiGate Administration Guide* and the *FortiGate Log Message Reference* for additional information.
- **Log search results enhancement** – You can now view log search results in both Format and Raw formats. See [“Searching the logs” on page 100](#) for more information.
- **Alert email configuration changes** – When configuring an alert email, you are now required to enter information in the alert name field, destination field, and device field and a drop-down list is included for selecting a destination. See [“Alert” on page 133](#) for more information.
- **Alert emails** – Alert emails now contain the FortiAnalyzer serial number in the Source Device field in the body of the email. The FortiAnalyzer serial number replaces the IP address of port 1 (FortiAnalyzer unit), which was used to identify the FortiAnalyzer unit that sent the alert email. See [“Alert” on page 133](#) for additional information about configuring alert emails.
- **SNMP enhancements** – When configuring SNMP communities in **Alert > Output > SNMP Access List**, you can now specify that traps for certain local system events will be generated that meet certain criteria. See [“Configuring SNMP traps and alerts” on page 136](#) for more information.
- **File directory menu** – You can now access all files that are on the FortiAnalyzer unit in **Tools > File Directory**. See [“File Explorer” on page 167](#) for more information.

3.0 MR7 new features and changes

The following descriptions includes only menus containing new features, changes to features, or both. Additional information is provided within this document.

Power supply monitoring for FortiAnalyzer-2000A and 4000A

In FortiAnalyzer 3.0 MR7, the new feature power supply monitoring provides a notification when a power supply fails or an administrator adds a power supply to the system. This notification is sent by the hardware monitoring daemon and in the following forms:

- Log – a log message is recorded at the system level
- Email – an email is sends out a critical event email message
- SNMP trap – a power supply event trap is sent

Both the web-based manager and CLI include settings for this new feature.

Registered devices' hard limits

In previous FortiAnalyzer 3.0 releases, the license limits of registered devices was reduced, causing those registered devices to not carry forward. The limit is now back to the maximum limit in FortiAnalyzer 3.0 MR4. This limit number prevents any loss of registered devices during upgrade. You can view the limits for registered devices on ["Maximum number of devices" on page 76](#) in the Device chapter.

CLI displays the tasks in the upload queue

A new diagnose command, `diagnose upload status`, has been added in FortiAnalyzer 3.0 MR7 for displaying files that are in the upload queue. Previously, in FortiAnalyzer 3.0 MR6, a queue maintained the upload's tasks but there was no way of verifying what was and what was not included in the queue.

Dashboard enhancements

The Dashboard contains nine new widgets in FortiAnalyzer 3.0 MR7. Administrators can have up to five tabs to the Dashboard as well.

Tabs allow administrators to customize what widgets display, for example, if administrators only need to view traffic widgets a tab can be configured so that it only displays all the traffic widgets.

The following are the new widgets that are available for display on the Dashboard:

- Log Receive Monitor
- RAID Monitor (if RAID is available on the FortiAnalyzer unit)
- Top Traffic
- Top Web Traffic
- Top Email Traffic
- Top FTP Traffic
- Top IM/P2P Traffic
- Virus Activity
- Intrusion Activity

For the Log Receive Monitor widget, a `diagnose` command will be introduced to provide information about total message rate, message rate per-protocol, and message rate per-device in the CLI.

See “System” on page 25 for information about the new widgets for FortiAnalyzer 3.0 MR7.

Custom fields for log messages

In FortiAnalyzer 3.0 MR7, you can now enable custom fields for log messages so that when the FortiAnalyzer unit receives these types of log messages, it can index them properly for reports or searching logs.

This feature is enabled only in the CLI using the following command syntax:

```
config log settings
    set custom-field<1-5>
```

The previous logs require re-indexing for this feature to be effective on them, and is only available in the CLI using the `diagnose log-indexer` command. This particular command can index per device and type, or all devices.

Reports

























Reports have been enhanced and modified for FortiAnalyzer 3.0 MR7. VoIP report charts were also included in FortiAnalyzer 3.0 MR7. These changes are also reflected in the CLI. See the *FortiAnalyzer CLI Reference* for additional information about the associated commands.

Report configuration enhancements

Report configuration has changed dramatically from FortiAnalyzer 3.0 MR6 to FortiAnalyzer 3.0 MR7. These changes are also reflected in the FortiGate unit's web-based manager and CLI. These dramatic changes do not affect previously configured reports in FortiAnalyzer 3.0 MR6 and earlier; however, you may want to reconfigure certain settings to simplify the previously configured reports.

These previously configured reports are separated based on what is included; for example, if DeviceSummary1_layout contains filters and output settings, the filters will be put in the Data Filter tab and given a name, and the output settings will be put in the Output tab and also given a name.

Figure 1: The previous FortiAnalyzer 3.0 MR6 reports, outlined in red, carried forward to FortiAnalyzer 3.0 MR7 and displayed in Layout with default report layouts

Create New		Delete			
<input type="checkbox"/>	Name	Description	Company Name	Number of Charts	
<input type="checkbox"/>	Bandwidth_Analysis	Overview of bandwidth consuming applications and users.		12	  
<input type="checkbox"/>	DeviceSummary_1_layout			360	  
<input type="checkbox"/>	Threat_Analysis	Overview of user Anti-Virus, Intrusion Protection and Anti-Spam threats for the time period.		13	  
<input type="checkbox"/>	Web_Filtering-Group_Activity	Overview of user website activity for a group of users. Provides summary and analysis information on usage patterns & behavior.		6	  
<input type="checkbox"/>	Web_Filtering-User_Activity	Overview of user website activity plus detailed audit of all blocked sites and all sites visited.		6	  
<input type="checkbox"/>	devicedetail_1_layout			1	  
<input type="checkbox"/>	usercontent_1_layout			22	  
<input type="checkbox"/>	usercontent_2_layout			16	  

Fortinet recommends configuring a test report layout and report schedule to familiarize yourself with how reports are configured in FortiAnalyzer 3.0 MR7. See [“Reports” on page 113](#) about how to configure reports in FortiAnalyzer 3.0 MR7.

In **Report > Config**, new tabs were added: Layout, Data Filter, Output, and Language. These new tabs allow you to configure multiple data filters, output destinations, report layouts (previously referred to as report profiles), and languages. The new menu, Schedule, provides settings and options for configuring a scheduled report.

Previously, you could configure specific report layouts such as Device Summary, Forensic, and User/Client report profiles. These report types were combined with other report types and removed from their respective tabs, which now provide greater flexibility for configuring report layouts. Forensic report options are now available when you select [Add Chart(s)] from the Chart List section of Report Layout.

Report schedules should be configured after configuring the report layout because you need to apply the report layout to the report schedules. Report schedules can also be configured from the FortiGate unit's web-based manager.

After configuring a report, you can generate that report immediately by selecting Run Now and view it in **Report > Browse**. You can also generate scheduled reports this way in **Report > Schedule**.

When viewing generated reports in Report Browse, the naming scheme is changed to the following:

- On-Demand-`<name of report>-<yyyy-mm-dd>-<time initiated by admin_hhmm>` – for reports that are generated immediately, for example:
On-Demand-Report_Headquarters-2008-06-03-0830
- `<name of scheduled report>-<yyyy-mm-dd>-<time_scheduled>` – all other reports, for example:
Report_Headquarters-2008-05-26-1030

These generated reports in Report Browse also contain only one rolled report when you expand a report. The name of rolled reports has changed as well and each is named after the section title that was configured in Layout. For example, if you had two section titles, Top Web Attacks and Top Viruses, the rolled reports would be named Top Web Attacks and Top Viruses. The default name for the rolled report is FortiAnalyzer Report. If generated reports carry forward from FortiAnalyzer 3.0 MR6, rolled reports might be renamed to the default name, FortiAnalyzer Report.

VoIP reports

VoIP activities and events are now available in reports. There are three log files that contain VoIP activity and event information: tlog.log, plog.log and clog.log. These log will be used for the following information:

- tlog.log – number of bytes pass per session
- plog.log – blocked VoIP activity
- clog.log – user registration information and call duration information

The individual reports that you select when configuring a report are available in the Fortinet Knowledge Center article, FortiAnalyzer Reports in 3.0 MR7, on the Fortinet Knowledge Center website.

Alert email configuration changes

When configuring an alert email in **Alert > Alert Event**, you now are required to enter information in the following fields:

- alert name
- destination (or destinations)
- device

Another configuration change is a drop-down list, providing the destinations of syslog servers, mail servers and SNMP access lists. The Syslog servers and SNMP access lists only display in the list when configured in **Alert > Output**.

Figure 2: The Destination drop-down list, circled, provides three destinations

The screenshot shows the 'Add Alert Event' configuration window. The 'Destination(s)' section is highlighted with a red circle, showing a dropdown menu with the following options: 'Please Select', '---- Email Address ----', 'mail.fortinet.com', '---- SNMP Server ----', 'test_123', '---- Syslog Server ----', and 'syslog_1'. The 'Add' and 'Delete' buttons are visible next to the dropdown.

Administrative Domains (ADOMs)

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

This section includes the following topics:

- [About administrative domains \(ADOMs\)](#)
- [Configuring ADOMs](#)

About administrative domains (ADOMs)

Enabling ADOMs alters the structure and available functionality of the web-based manager and CLI according to whether you are logging in as the `admin` administrator, and, if you are not logging in as the `admin` administrator, the administrator account's assigned access profile.

Table 1: Characteristics of the CLI and web-based manager when ADOMs are enabled

	<code>admin</code> administrator account	Other administrators
Access to Global Configuration	Yes	No
Access to Administrative Domain Configuration (can create ADOMs)	Yes	No
Can create administrator accounts	Yes	No
Can enter all ADOMs	Yes	No

Table 2: Configuration locations when ADOMs are enabled

Within Global Configuration:	Within each ADOM:
System > Dashboard (includes tabs, if configured) System > Network > Interface System > Network > DNS System > Network > Routing System > Admin > Administrator System > Admin > Access Profile System > Admin > Auth Group System > Admin > RADIUS Server System > Admin > Settings System > Admin > Monitor System > Network Sharing > Windows Share System > Network Sharing > NFS Export System > Network Sharing > User System > Network Sharing > Group System > Config > Log Setting System > Config > Log Aggregation System > Config > Log Forwarding System > Config > RAID System > Maintenance > Backup & Restore System > Maintenance > FortiGuard Center Device > All > Device (devices assigned to an ADOM other than <code>root</code> cannot be deleted) Device > All > Blocked Device Log > Config > Log Config Report > Config > Language Quarantine > Config > Quarantine Config Alert > Alert Event > Alert Event Alert > Output > SNMP Access List Alert > Output > Syslog Server Tools > Vulnerability Scan > Module Tools > File Explorer > File Explorer	System > Config > IP Alias System > Config > LDAP Device > All > Device (read only) Device > All > Group Log > Log Viewer > Real-time Log > Log Viewer > Historical Log > Search > Log Search Log > Browse > Log Browser Content Archive > Web Archive Content Archive > Email Archive Content Archive > File Transfer Content Archive > IM Chat Content Archive > VoIP Archive Report > Browse > Result Report > Schedule > Schedule Report > Config > Layout Report > Config > Data Filter Report > Config > Output Quarantine > Repository > Repository Alert > Output > Mail Server Tools > Vulnerability Scan > Job Tools > Vulnerability Scan > Report Tools > File Explorer > File Explorer

- If ADOMs are enabled and you log in as `admin`, you first access Administration Domain Configuration. A superset of the typical menus and CLI commands appear, allowing unrestricted access and ADOM configuration.
 - Global Configuration contains settings used by the FortiAnalyzer unit itself and settings shared by ADOMs, such as the device list, RAID, and administrator accounts. It does not include ADOM-specific settings or data, such as logs and reports. When configuring other administrator accounts, an additional option appears allowing you to restrict other administrators to an ADOM.
If you enter Global Configuration, a Main Menu item appears in the menu, enabling you to return to the top level menu area, Administrative Domain Configuration.
 - Administrative Domains allows you to configure or access ADOMs. You can add a device to one or more ADOMs. If you enter an ADOM, a Main Menu item appears in the menu, enabling you to return to the top level menu area, Administrative Domain Configuration.

- If ADOMs are enabled and you log in as any other administrator, you enter the ADOM assigned to your account. A subset of the typical menus or CLI commands appear, allowing access only to only logs, reports, quarantine files, content archives, IP aliases, and LDAP queries specific to your ADOM. You cannot access Global Configuration, or enter other ADOMs.

By default, administrator accounts other than the `admin` account are assigned to the `root` ADOM, which includes all devices in the device list. By creating ADOMs that contain a subset of devices in the device list, and assigning them to administrator accounts, you can restrict other administrator accounts to a subset of the FortiAnalyzer unit's total devices or VDOMs.

The `admin` administrator account cannot be restricted to an ADOM. Other administrators are restricted to their ADOM, and cannot configure ADOMs or Global Configuration.

The maximum number of ADOMs varies by FortiAnalyzer model.

FortiAnalyzer Model	Number of Administrative Domains
FortiAnalyzer-400	10
FortiAnalyzer-800/800B	50
FortiAnalyzer-2000/2000A	100
FortiAnalyzer-4000/4000A	250



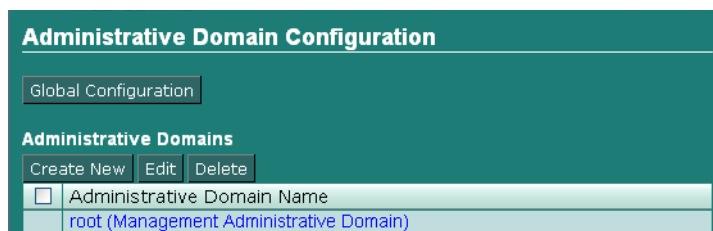
Note: ADOMs are not available on the FortiAnalyzer-100 or FortiAnalyzer-100A/100B.

The `admin` administrator can further restrict other administrators' access to specific configuration areas within their ADOM by using access profiles. For more information, see ["Access Profile" on page 50](#)

Configuring ADOMs

Administrative domains (ADOMs) are disabled by default. To use administrative domains, the `admin` administrator must first enable the feature, create ADOMs, and assign other FortiAnalyzer administrators to an ADOM.

Figure 1: Administrative Domain Configuration



Global Configuration The `admin` administrator can access the global configuration. Select Main Menu to return to the Admin Domain Configuration page.

Create New Select to create a new ADOM.

Edit Select an ADOM's check box, then select Edit to change the name or member devices and VDOMs of the selected ADOM.

Delete Select an ADOM's check box, then select Delete to remove the selected ADOM.

Name Select a name to enter that ADOM. Select Main Menu to return to Admin Domain Configuration.



Caution: Enabling ADOMs moves non-global configuration items to the `root` ADOM. Back up the FortiAnalyzer unit configuration before beginning the following procedure, to enable ADOMs. For more information about backing up your configuration, see [“Backup & Restore” on page 69](#).

To enable ADOMs

- 1 Log in as `admin`.
Other administrators cannot enable, disable, or configure ADOMs.
- 2 Go to **System > Admin > Settings**.
- 3 Enable Admin Domain Configuration.
- 4 Select OK.

A message appears:

Enabling/Disabling the admin domain configuration will require you to re-login. Are you sure you want to continue?

- 5 Select OK.
The FortiAnalyzer unit logs you out.
- 6 To confirm that ADOMs are enabled, log in as `admin`.

Administrative Domain Configuration appears, providing access to both Global Configuration and ADOM configuration. See [“To add or edit an ADOM” on page 22](#) to create ADOMs. See [“Assigning administrators to an ADOM” on page 24](#) to assign an administrator to an ADOM.

To add or edit an ADOM

- 1 Log in as `admin`.
Other administrators cannot enable, disable, or configure ADOMs.
- 2 Select Create New, or select the check box next to an ADOM and select Edit.
- 3 Enter a Name for the ADOM.
- 4 Select which devices to associate with the ADOM from Available Devices, then select the right arrow to move them to Selected Devices.

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

To remove a device from Selected Devices, select one or more devices, then select the left arrow to move them to Available Devices.

- 5 If the ADOM includes a FortiGate unit and you want to restrict the ADOM to a specific VDOM, enable Restrict to a FortiGate VDOM, then enter the VDOM name.
- 6 Select OK.



Caution: Deleting ADOMs, which can occur when disabling the ADOM feature, removes administrator accounts assigned to ADOMs other than the `root` ADOM. Back up the FortiAnalyzer unit configuration before beginning this procedure. For more information, see ["Backup & Restore" on page 69](#).

If you do not wish to delete those administrator accounts, assign them to the `root` ADOM before disabling ADOMs.

To disable ADOMs

- 1 Log in as `admin`.
Other administrators cannot enable, disable, or configure ADOMs.
- 2 Select the check boxes next to each ADOM except the `root` (Management Administrative Domain) ADOM, then select Delete.
If any other ADOMs except the `root` ADOM remain, the option to disable ADOMs will not appear.

- 3 Go to **Global Configuration > System > Admin > Settings**.
- 4 Disable Admin Domain Configuration.
- 5 Select OK.

A message appears:

Enabling/Disabling the admin domain configuration will require you to re-login. Are you sure you want to continue?

- 6 Select OK.
The FortiAnalyzer unit logs you out.

Accessing ADOMs as the `admin` administrator

When ADOMs are enabled, additional ADOM items become available to the `admin` administrator and the structure of the web-based manager menu changes. After logging in, other administrators implicitly access the subset of the web-based manager that pertains only to their ADOM, while the `admin` administrator accesses the root of the web-based manager and can use all menus. The `admin` administrator must explicitly enter the part of the web-based manager that contains an ADOM's settings and data to configure items specific to an ADOM.

To access an ADOM

- 1 Log in as `admin`.

Other administrators can access only the ADOM assigned to their account.

- 2 In the Administrative Domains area, select the name of the ADOM you want to enter.

The ADOM-specific menu subset appears. While in this menu subset, any changes you make affect this ADOM only, and do not affect devices in other ADOMs or global FortiAnalyzer unit settings.

You can return to Administrative Domain Configuration by going to **Main Menu**.

Assigning administrators to an ADOM

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



Note: By default, when ADOMs are enabled, existing administrator accounts other than `admin` are assigned to the `root` ADOM, which contains all devices in the device list. For more information about creating other ADOMs, see [“Configuring ADOMs” on page 22](#).

To assign an administrator to an ADOM

- 1 Log in as `admin`.

Other administrators cannot configure administrator accounts when ADOMs are enabled.

- 2 Go to **Global Configuration > System > Admin > Administrator**.

- 3 Configure the administrator account as described in [“Adding or editing an administrator account” on page 49](#), selecting the Admin Domain that the administrator will be able to access.

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

System

The System menu contains basic FortiAnalyzer unit system settings, such as network interfaces, DNS, routing, local logging, administrators, and network shares, and displays system statistics and provides basic system operations from the Dashboard. From the System menu, you can also back up or restore a configuration, or update the firmware on the FortiAnalyzer unit.

This section includes the following topics:

- [Dashboard](#)
- [Network](#)
- [Admin](#)
- [Network Sharing](#)
- [Config](#)
- [Maintenance](#)

Dashboard

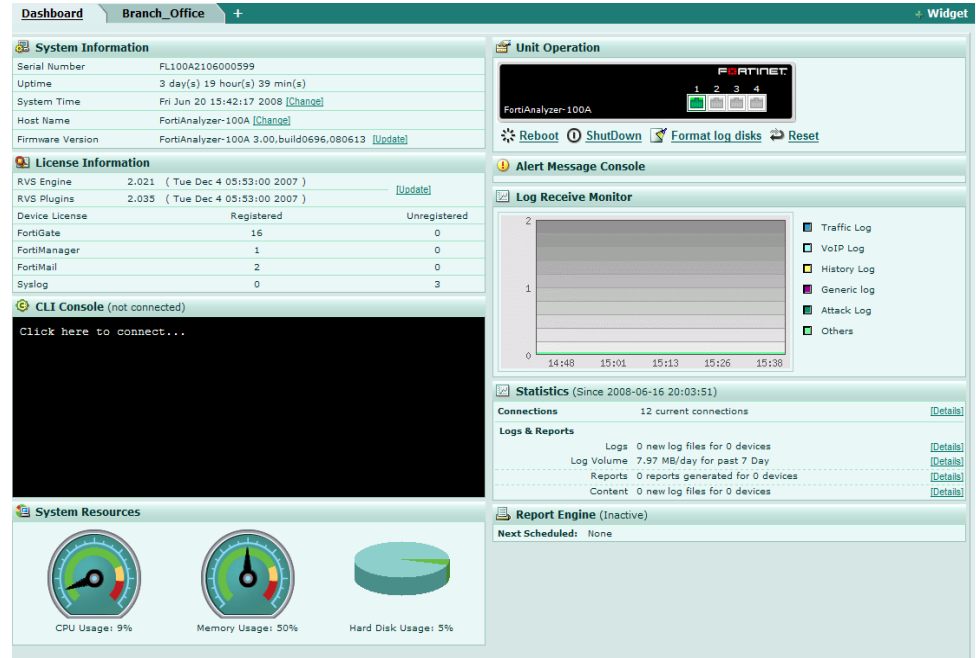
Dashboard provides a summary view of the current operating status of the FortiAnalyzer unit, including any additional information happening on the network, such as top attacks or what types of logs were received.

The Dashboard also provides tabs so that you can customize different widget displays. For example, if administrators want to view only traffic activity, a tab called Traffic Activity would be added to the Dashboard with only the traffic activity widgets displaying on that tab.

The following widgets are available on the Dashboard:

- System Information
- License Information
- CLI Console
- System Resources
- System Operation
- Alert Message Console
- Statistics
- Report Engine
- RAID Monitor
- Log Receive Monitor
- Virus Activity
- Intrusion Activity
- Top Traffic
- Top FTP Traffic
- Top Email Traffic
- Top Web Traffic
- Top IM/P2P Traffic

Figure 1: Dashboard of a FortiAnalyzer-100A unit displaying one of the new widgets Log Receive Monitor and a tab, Branch Office



To rearrange a Dashboard widget

- 1 Go to **System > Dashboard**.
- 2 Place your mouse cursor over the widget's title bar area, but not over buttons such as Hide or Close.

The cursor changes to a multidirectional arrow.

- 3 Select and drag the widget to its new location.

While dragging the widget, a red dashed line outlines the widget's current destination, and other widgets reposition themselves to display the resulting layout.

To refresh a Dashboard widget

- 1 Go to **System > Dashboard**.
- 2 Place your mouse cursor over the widget's title bar area.
Refresh Now appears on the right side of the title bar.
- 3 Select Refresh Now.

The widget refreshes with current data.

To minimize or expand a Dashboard widget

- 1 Go to **System > Dashboard**.
- 2 Place your mouse cursor over the widget's icon, located on the right side of the title bar area.
 - If the widget is currently minimized, the arrow appears on its side, pointing to the right.
 - If the widget is currently expanded, the arrow appears pointing downward.

- 3 Select Show or Hide.
The widget toggles between showing the full widget and being minimized to show only its title bar.

To include a Dashboard widget

- 1 Go to **System > Dashboard**.
- 2 Select "+ Widget".
- 3 A widget selection overlay appears.
- 4 Select one or more widgets. Alternatively, to restore the default set of widgets, select Back to Default.
The selected widgets appear on the Dashboard layout. Widgets whose names are gray are already included on the Dashboard layout, and cannot be included more than once.
- 5 Select "X" in the upper right corner.
The widget selection overlay closes.

To omit a Dashboard widget

- 1 Go to **System > Dashboard**.
- 2 Place your mouse cursor over the widget's title bar area.
Close appears on the right side of the title bar.
- 3 Select Close.
A confirmation dialog appears.
- 4 Select OK.
The widget is removed from the Dashboard layout.

Tabs

Tabs provide a way to customize what widgets administrators view, for example, administrators only need to view traffic widgets. You can add, delete, or rename tabs.

When adding widgets to tabs, you cannot have duplicate widgets on multiple tabs. For example, if you have the RAID Monitor widget in the Dashboard and you want to add the same widget to your new tab, Office_1, the RAID Monitor widget will only display in the Dashboard.

To add a tab

- 1 Go to **System > Dashboard**.
- 2 Select the plus (+) symbol beside the Dashboard tab.
- 3 Enter a name for the new tab.
- 4 Select +Widget to add the widgets you want to the new tab.
- 5 If applicable, edit the widgets to customize what each displays.

To rename a tab

- 1 Go to **System > Dashboard**.
- 2 Double-click on the name of the tab and press Delete.

- 3 Enter a new name and press Enter.

To delete a tab

- 1 Go to **System > Dashboard**.
- 2 Double-click on the name of the tab and select the (X) symbol.

RAID Monitor

The RAID Monitor area of the Dashboard displays information about the status of RAID disks as well as what RAID level has been selected. The RAID Monitor also displays how much disk space is being used.

The RAID Monitor layout is similar to the look of the front panel. The Device Status Indicator allows you to view each disk's name and the amount of space in GB each has. For example, Disk 2: Ready 465.76GB.

You can configure RAID settings from the RAID Monitor area as well by selecting RAID Settings. This option is only available when you move your mouse over the title bar.

Figure 2: RAID Monitor displaying a RAID array without any failures

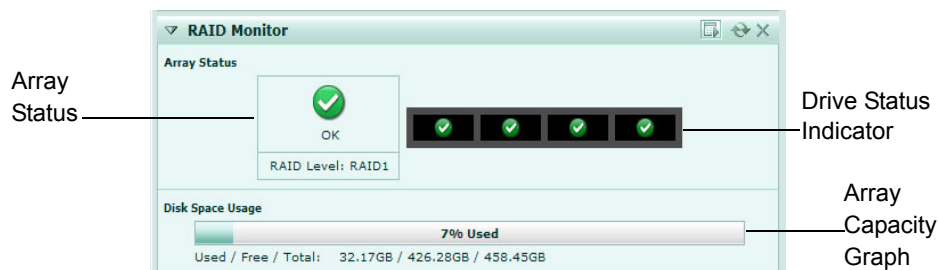
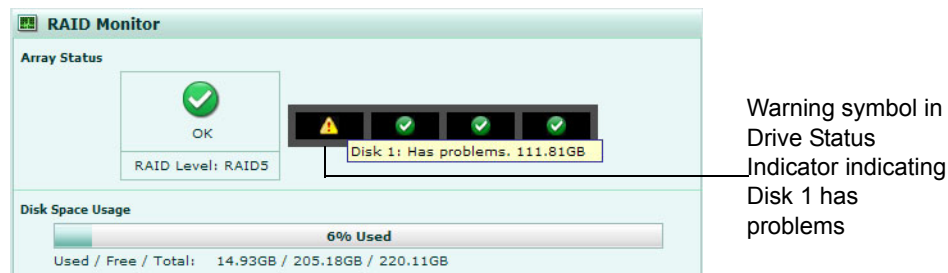
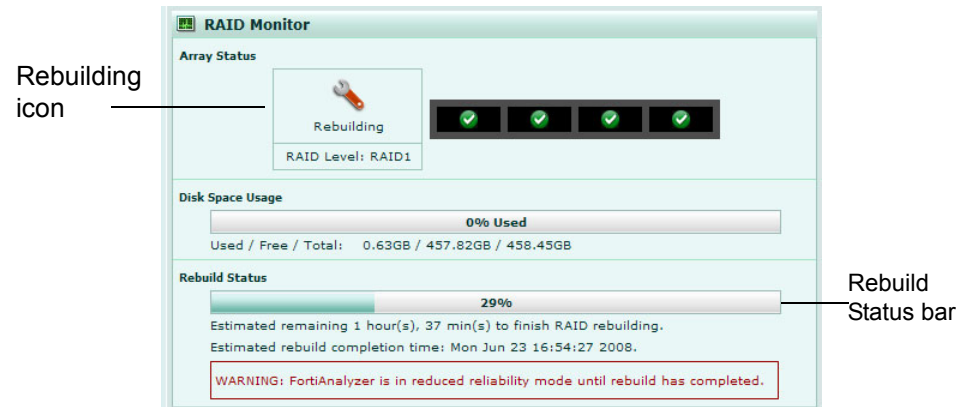


Figure 3: RAID Monitor displaying a failed disk



In Figure 5, the Drive Status Indicator is indicating that Disk 1 has problems. This is displayed by both a warning symbol and text. The text appears when you hover your mouse over the warning symbol; the text also indicates the amount of space in GB. When a disk has failed, a circle with an X appears in Drive Status Indicator.

Figure 4: RAID Monitor displaying a disk that is being rebuilt



Array Status

Displays the following icons and status text when the RAID disk is okay, failed or being rebuilt:

- green checkmark (OK) – indicates that the RAID disk has no problems
- warning symbol (Warning) – indicates that there is a problem with the RAID disk, such as a failure, and needs replacing. The RAID disk is also in reduced reliability mode when this status is indicated in the widget.
- wrench symbol (Rebuilding) – indicates that a drive has been replaced and the RAID array is being rebuilt; it is also in reduced reliability mode
- exclamation point (Failure) – indicates that multiple drives have failed and the RAID array is corrupted and that the drive must be reinitialized

Disk space usage

Displays the amount of disk used in both percentage and a fill line.

Used/Free/Total

Displays the amount of used disk space, available or free disk space, and the total available disk space. These numbers are displayed in GB.

Rebuild Status progress bar

A bar indicating the progress of the rebuilding of a RAID array. This bar displays the progress in percent. This bar displays only when a RAID array is being rebuilt.

Estimated rebuild time

[start and end time] (For software RAID only)

The time period of when the rebuild will be complete. The time is displayed by the number of hours, minutes and seconds. The time period also indicates when the rebuilding process will end, displaying the name of the day, and the time in 12-hour format, for example, Friday at 3:14 pm.

This time period displays only when an array is being rebuilt.

This time period will not display in hardware RAID, such as FortiAnalyzer-2000/2000A, and FortiAnalyzer-4000/4000A.

Rebuild Warning

A bar and text reminding you the system has no redundancy protection until the rebuilding process is complete. This text displays only when an array is being rebuilt.

System Information

The System Information area of the Dashboard displays basic information about the FortiAnalyzer unit, such as up time and firmware version.

Figure 5: System Information

System Information	
Serial Number	FL100A2106000599
Uptime	24 day(s) 20 hour(s) 8 min(s)
System Time	Tue Oct 9 17:19:40 2007 [Change]
Host Name	FortiAnalyzer-100A [Change]
Firmware Version	FortiAnalyzer-100A 3.00,build615,070828 [Update]

- Serial Number** The serial number of the FortiAnalyzer unit. The serial number is unique to the FortiAnalyzer unit and does not change with firmware updates. Use this number when registering your FortiAnalyzer unit with Fortinet.
- Uptime** The time in days, hours and minutes since the FortiAnalyzer was started or last rebooted.
- System Time** The current time according to the FortiAnalyzer internal clock. Select Change to change the time or configure the FortiAnalyzer unit to obtain the time from an NTP server. For more information, see [“Setting the time” on page 29](#).
- Host Name** The name of the FortiAnalyzer unit. For more information about changing the name, see [“Changing the host name” on page 30](#).
- Firmware Version** The version of the firmware installed on the FortiAnalyzer unit. Select Update to upload a new version of the firmware. For more information about updating the firmware, see [“Changing the firmware” on page 30](#).

Setting the time

Set the system time to ensure correct report time ranges and scheduling and accurate logging. You can either manually set the FortiAnalyzer system time or you can configure the FortiAnalyzer unit to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.

To set the system time, go to **System > Dashboard** and select Change for the System Time.

Figure 6: Time Settings

- System Time** The current FortiAnalyzer system date and time.
- Refresh** Update the display of the current FortiAnalyzer system date and time.
- Time Zone** Select the FortiAnalyzer unit’s time zone.
- Set Time** Select to set the FortiAnalyzer system date and time to the values you set in the Year, Month, Day, Hour, Minute and Second fields. Alternatively, select Synchronize with NTP Server.

Synchronize with NTP Server	Select to use an NTP server to automatically set the system date and time. You must specify the server and synchronization interval. Alternatively, select Set Time.
Server	Enter the IP address or domain name of an NTP server. See http://www.ntp.org to find an NTP server that you can use.
Sync Interval	Specify how often the FortiAnalyzer unit should synchronize its time with the NTP server. For example, a setting of 1440 minutes causes the FortiAnalyzer unit to synchronize its time once a day.

Changing the host name

Change the FortiAnalyzer host name to differentiate the FortiAnalyzer from other FortiAnalyzer units or other devices on your network.

To change the host name

- 1 Go to **System > Dashboard**.
- 2 In the System Information area, select Change for the Host Name.
- 3 Enter a new name for the FortiAnalyzer unit.
- 4 Select OK.

Changing the firmware

A FortiAnalyzer unit may be upgraded to a newer firmware version, or reverted to a previous firmware version by selecting Update in System Information. For more information about changing the firmware in the web-based manager, see [“Managing firmware versions” on page 169](#).

License Information

The License Information area of the Dashboard displays information on features that vary by a purchased license or contract.

For more information about RVS (remote vulnerability scanning) updates, see [“FortiGuard Center” on page 70](#).

Figure 7: License Information

License Information		
RVS Engine	2.019 (Sun Mar 18 20:50:00 2007)	[Update]
RVS Plugins	2.029 (Fri Jun 1 01:38:00 2007)	
Device License	Registered	Unregistered
FortiGate	7	0
FortiManager	1	0
FortiMail	1	0
Syslog	1	0

RVS Engine

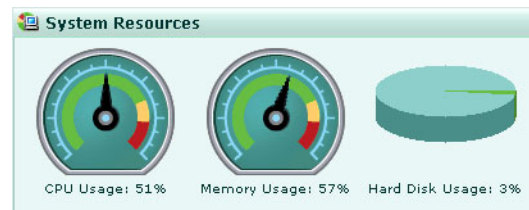
The version of the RVS engine, and the date of its last update. Select Update to upload a new version of the engine. For more information on RVS, see [“FortiGuard Center” on page 70](#). This feature is not available on the FortiAnalyzer-100.

RVS Plug-ins	The version of the RVS plug-in, and the date of its last update. This feature is not available on the FortiAnalyzer-100.
Device License	<p>A total of the number of each device type connecting or attempting to connect to the FortiAnalyzer unit. For more information about the maximum numbers of devices of each type and/or VDOMs that are permitted to connect to the FortiAnalyzer unit, see “Maximum number of devices” on page 76.</p> <ul style="list-style-type: none"> Registered is the number of devices that you have added to the FortiAnalyzer unit’s device list, either manually or automatically. Unregistered is the number of devices attempting to connect to the FortiAnalyzer unit that are not yet registered. To configure the FortiAnalyzer unit to accept data from a device, see “Manually adding a device” on page 80.

System Resources

The System Resources area of the Dashboard displays use of the FortiAnalyzer unit’s resources, including CPU, memory (RAM) and hard disk.

Figure 8: System Resources



CPU Usage	The current CPU usage status. The web-based manager displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.
Memory Usage	The current memory status. The web-based manager displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.
Hard Disk Usage / RAID status	<p>For the FortiAnalyzer-100 and FortiAnalyzer-100A/100B, the current status of the hard disk. The web-based manager displays the amount of hard disk space used.</p> <p>For the FortiAnalyzer-400, FortiAnalyzer-800/800B, FortiAnalyzer-2000/2000A and FortiAnalyzer-4000/4000A, the current RAID status of the hard disks. Each circle indicates the status of a hard disk. Green indicates the hard disk is functioning normally. If the disk is flashing red and yellow, there is a problem with the hard disk.</p> <p>The hard disks on the FortiAnalyzer-2000/2000A and FortiAnalyzer-4000/4000A are hot swappable. For more information, see “Hot swapping the FortiAnalyzer-2000/2000A and FortiAnalyzer-4000/4000A” on page 66.</p>
History icon	Select History, which appears when placing the mouse cursor over the title bar, to view a graphical representation of the last minute of CPU, memory, sessions, and network usage. For more information, see “Viewing operational history” on page 32 .

Viewing operational history

The System resource history page displays four graphs representing system resources and network utilization history, updated every three seconds.

To view the FortiAnalyzer operational history

- 1 Go to **System > Dashboard**.
- 2 Select History in the upper right corner of the System Resources area.

CPU Usage	The CPU usages for the previous minute.
Memory Usage	The memory usages for the previous minute.
Session	The session history for the previous minute.
Network Utilization	The network use for the previous minute.

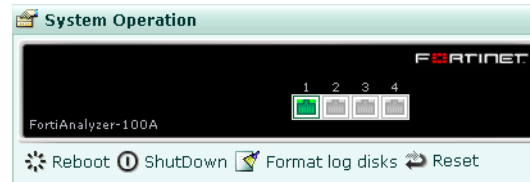
System Operation

Some basic operations can be performed directly from the Dashboard in the System Operation area.



Note: These operations are available only to users with the read and write access profile.

Figure 9: System Operation



Reboot	Restart the FortiAnalyzer unit.
ShutDown	Halt all processes on the FortiAnalyzer unit in preparation to power off the hardware. To restart the FortiAnalyzer unit after shutdown, perform a power cycle.
Format log disks	Format the FortiAnalyzer hard disk. Selecting this option will delete all log files and reports from the hard disk. Ensure that you back up all information before selecting this option. Formatting the hard disk will also interrupt FortiAnalyzer operations for several minutes.
Reset to factory default	Reset the FortiAnalyzer unit to the default configuration for its firmware version. Caution: This option resets all FortiAnalyzer settings to their default state. This includes the interface IP addresses, as well as HTTP, HTTPS, SSH, and Telnet access. You will need to reconnect to the FortiAnalyzer device using the default IP address of 192.168.1.99.

Formatting the log disks

You can use the system dashboard to format the FortiAnalyzer log disks. Remember to back up and log data before formatting the hard disks. The FortiAnalyzer unit will be unavailable for the duration of the format process.

To format the log disks

- 1 Go to **System > Dashboard**.
- 2 In the Systems Operations area, select Format Log Disks.
- 3 Select OK.

Resetting to the default configuration

You can reset the FortiAnalyzer unit to its default configuration.

Resetting the configuration does not restore the original firmware. Configuration and firmware are distinct. Use the procedures in [“Managing firmware versions” on page 169](#) for managing firmware.



Caution: Back up the configuration before resetting. Resetting the configuration deletes all changes you have made to the FortiAnalyzer configuration, reverting it to the firmware’s default configuration, including resetting interface IP addresses.

To reset to the default configuration

- 1 Go to **System > Dashboard**.
- 2 In the System Operations area, select Reset.
- 3 Select OK to confirm.

The FortiAnalyzer unit restarts with the default configuration for the currently installed firmware version.

Alert Message Console

The Alert Message Console displays alert messages for the FortiAnalyzer unit and connected devices, including hard disk failure messages, virus outbreak, or suspicious event warnings.

To set the threshold for Alert Message Console, or to view all the alert messages recorded by the FortiAnalyzer unit, select More alerts. For more information about viewing alert messages, see [“Viewing alert console messages” on page 34](#).

Viewing alert console messages

Alert console messages provides a window on what is occurring on the FortiAnalyzer and other FortiGate devices. These messages allow you to view issues on your network, including network attacks and virus warnings.

The Alert messages window provides a complete list of alert messages. You can view the alert messages by level or acknowledge the messages as required. Acknowledging an alert message removes it from the list of alerts.

Alert messages can also be delivered by email, Syslog or SNMP. For more information, see [“Alert Events” on page 133](#).

To view alert console messages

- 1 Go to **System > Dashboard**.
- 2 Select More Alerts in the upper right corner of the Alert Message Console area.
- 3 Select the column headers to sort the column in ascending or descending order.

Figure 10: Alert messages

Acknowledge					
1 of 1		Include Warning and higher	Keep Unacknowledged Alerts for 7 days	formatted raw	
<input type="checkbox"/>	Device	Event	Severity	Time	Counter
<input type="checkbox"/>	FortiManager-3000	"FWMANAGER (1236): DES=LOGTP_LINKD:main: Start firmware manager linkd process...."	Alert	Wed Apr 25 17:00:26 2007	1
<input type="checkbox"/>	FortiManager-3000	"FWMANAGER (1237): DES=LOGTP_FMUPD:main: starting_firmware manager schedule upgrade process....."	Alert	Wed Apr 25 17:00:26 2007	1
<input type="checkbox"/>	Local FortiAnalyzer	"Invalid default gateway address"	Alert	Wed Apr 25 15:21:25 2007	1
<input type="checkbox"/>	FortiManager-3000	"FWMANAGER (1235): DES=LOGTP_LINKD:main: Start firmware manager linkd process...."	Alert	Wed Apr 25 10:07:14 2007	1
<input type="checkbox"/>	FortiManager-3000	"FWMANAGER (1236): DES=LOGTP_COMM:netcom_socket_connect: Failed to connect to socket. err: 101(Network is unreachable)"	Error	Thu Apr 26 09:33:43 2007	95
<input type="checkbox"/>	FortiManager-3000	"FWMANAGER (1236): DES=FCP_connect: FR_conn_connect failed. ret:-1046. err:101(Network is unreachable)"	Error	Thu Apr 26 09:33:43 2007	95
<input type="checkbox"/>	FortiManager-3000	"FWMANAGER (1236): DES=LOGTP_COMM:linkdlib_send_and_recv: Failed to connect to fds server: fds1.fortinet.com:443"	Error	Thu Apr 26 09:33:43 2007	95
<input type="checkbox"/>	Local FortiAnalyzer	"Send mail to SMTP server mail.example.com failed."	Warning	Thu Apr 26 09:30:32 2007	360

Page	Select the page of alerts to view. Use the arrows to move forward and back through the pages or enter a page number and press Enter.
Include...and higher	Select an alert level to view. The level you select and those alert messages higher than selected will appear in the alert list.
Keep Unacknowledged Alerts for	Select the number of previous days of alert messages to display. Selecting a number of days lower than what you are currently viewing deletes the older alerts. For example, if you are viewing alerts for seven days, and change the alerts to two days, the FortiAnalyzer unit deletes the other five days of alert messages.
formatted raw	Select to view the alert messages in a formatted or raw format.
Device	The device where the alert message is originating.
Event	Details of the event causing the alert message.
Severity	The level of the alert message.
Time	The date and time of the alert message.
Counter	The number of occurrences of the alert event.
Delete	Select the check box for alert messages you want to delete, then select the delete icon.

Statistics

The Statistics area of the Dashboard counts the numbers of sessions, logs, and reports handled by the FortiAnalyzer unit.

Figure 11: Statistics

Statistics (Since 2007-10-09 17:29:42)		
Connections	74 current connections	[Details]
Logs & Reports		
Logs	0 new log files for 0 devices	[Details]
Log Volume	21.44 MB/day for past 7 day(s)	[Details]
Reports	1 reports generated for 1 devices	[Details]
Content	0 new log files for 0 devices	[Details]

Since	The date and time when the statistics were last reset.
Connections	The number of communication sessions occurring on the FortiAnalyzer unit. Select Details for more information on the connections. For more information about the session information, see "Viewing session information" on page 35 . For administrative sessions only, see "Monitor" on page 52 .
Logs & Reports	The log file volume received per day.

Viewing session information

Session information displays information about the current communications sessions on the FortiAnalyzer unit, including devices that connect to send logs or quarantine files.

To view the session information

- 1 Go to **System > Dashboard**.
- 2 In the Statistics area, next to Connections, select Details.

Resolve Host Name	Select to display host names by a recognizable name rather than IP addresses. For more information about on configuring IP address host names see “Configuring IP aliases” on page 60 .
Resolve Service	Select to display network service names rather than port numbers, such as HTTP rather than port 80.
Refresh Time	Select the frequency of the refresh of the Connections page to view the connection activity.
Stop Refresh	When the refresh is started, select to stop the refreshing of the connections page. To re-start the refresh, select Start Refresh.
Start Refresh	When the refresh is stopped, select to start the refreshing of the connections page. To stop the refresh, select Stop Refresh.
View <i>n</i> per page	Select the number of rows to display per page.
Page <i>n</i> of <i>n</i>	Enter a page number, then press Enter to go to the page.
Search	Enter a keyword to perform a simple search on the session information available. Select Go to begin the search. The number of matches appears above the Search field.
Protocol	The service protocol of the connection, such as UDP or TCP.
From IP	The source IP address of the connection.
From Port	The source port of the connection.
To IP	The destination IP address of the connection.
To Port	The destination port of the connection.
Expires (Secs)	The time in seconds remaining before the connection terminates.

Filtering session information

You can filter the contents to find specific content. Each column of data includes a gray filter icon. Select the icon to filter the contents of the column.

When applying a column filter, the filter icon appears green.

To turn off the filter, select the filter icon for the column, and select Clear all Filters.

Report Engine

The Report Engine display shows the FortiAnalyzer report generation activity. The report engine activity information includes whether the report engine is active or inactive, what reports are running when active and the percentage completed.

Select the Generate report button to create a new report profile.

Figure 12: Report Engine



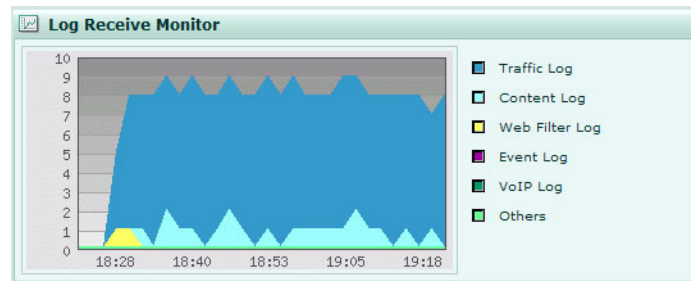
Log Receive Monitor

The Log Receive Monitor displays historical analysis of the rate at which logs are received. This widget displays this information in a graphical format.

You can display information by the type of logs or by device and you can also specify the time period. A new `diagnose` command was also added to display this information in the CLI.

You can edit the Log Receive Monitor to display specific information. The following procedure describes how to edit the Log Receive Monitor widget.

Figure 13: Log Receive Monitor widget



To edit information for Log Receive Monitor

- 1 Go to **System > Dashboard**.
- 2 On the Log Receive Monitor, select Edit in the title bar area.
- 3 Enter the appropriate information for the following:

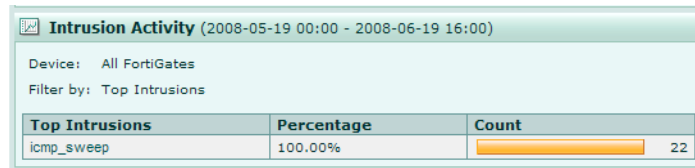
Type	Select either Log Type or Device. If you choose Log Type, the monitor displays the type of logs that are received from all registered devices and separates them into categories, for example top 5 traffic logs, antivirus logs. If you choose Device, the monitor displays the logs that received by each registered device and separates the devices into the top number of devices.
Top N	Select one number from the drop-down list to display the top log types. If you select only one number from the drop-down list, only the top log type will display, for example, the traffic log.
Period	The time range for monitoring the logs received. You can select one of the following: <ul style="list-style-type: none"> • Hour – monitors the rate at which logs are received within a period of one hour • Day – monitors the rate at which logs are received within a period of one day • Week – monitors the rate at which logs are received within a period of one week
Automatically Refresh	Select the check box if you want to have the monitor automatically refresh the information.
- 4 Select OK.

Intrusion Activity

Intrusion Activity displays the top attacks that occurred on the network. This information is gathered from attack logs.

You can edit the Intrusion Activity widget to display specific information by using the following procedure.

Figure 14: Intrusion Activity widget



To edit the information for Intrusion Activity

- 1 Go to **System > Dashboard**.
- 2 In Intrusion Activity, select Edit in the title bar area.
- 3 Enter the appropriate information for the following:
 - Device** Select the registered device or device group from the drop-down list.
 - Display by** Select one of the following to filter the log information:
 - Top Sources (to any) – filters any top source IP addresses
 - Top Destinations (from any) – filters any top destination IP addresses
 - Top Intrusions – filters the top intrusion activity
 - Time Period – filters the top intrusion activity by period of time, from 00:00:00 to 23:59:59 (24 hours).
 - Time Scope** Select one of the following for the time range:
 - Hour – filters the time by hour
 - Day – filters the time by the current day
 - Week – filters the time by the current week
 - Month – filters the time by the current month
 - No. Entries** Select the number of entries to display. For example, if you want to display 10 entries, select 10 from the drop-down list. You can specify only 5, 10, or 20.

- 4 Select OK.

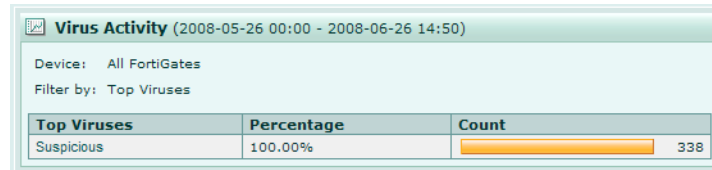
You can view the log messages that are associated with the information that displays in Intrusion Activity by selecting the links.

Virus Activity

Virus Activity displays the virus activity that has occurred on the devices. This information is gathered from virus logs. You can edit Virus Activity to display specific information.

The following procedure describes how to edit the Virus Activity widget.

Figure 15: Virus Activity widget



To edit the information for Virus Activity

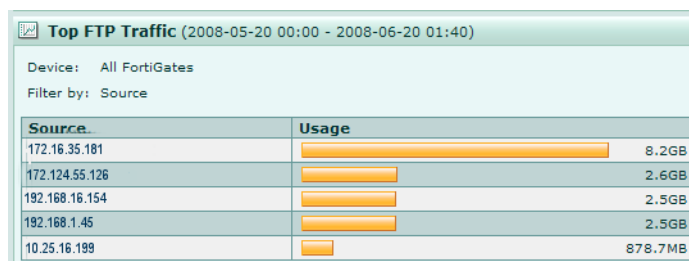
- 1 Go to **System > Dashboard**.
- 2 In Virus Activity, select Edit in the title bar area.
- 3 Enter the appropriate information for the following:
 - Device** Select the registered device or device group from the drop-down list.
 - Display by** Select one of the following to filter the information:
 - Time Period – filters virus activity by time period
 - Top Viruses – filters top virus activity only
 - Top Sources (to any) – filters top sources
 - Top Destinations (from any) – filters top destinations
 - Protocol break down for virus incidents – filters by protocol
 - Time Scope** Select one of the following for the time range:
 - Hour – filters the time by hour
 - Day – filters the time by the current day
 - Week – filters the time by the current week
 - Month – filters the time by the current month
 - No. Entries** Select the number of entries to display. For example, if you want to display 10 entries, select 10 from the drop-down list. You can specify only 5, 10, or 20.
- 4 Select OK.

Top FTP Traffic

Top FTP Traffic displays the total amount of file transfers that occur, using a bar chart. This information is gathered from traffic logs.

You can edit Top FTP Traffic to customize the information that displays. The following procedure describes how to edit the Top FTP Traffic widget.

Figure 16: Top FTP Traffic widget



To edit the information for Top FTP Traffic

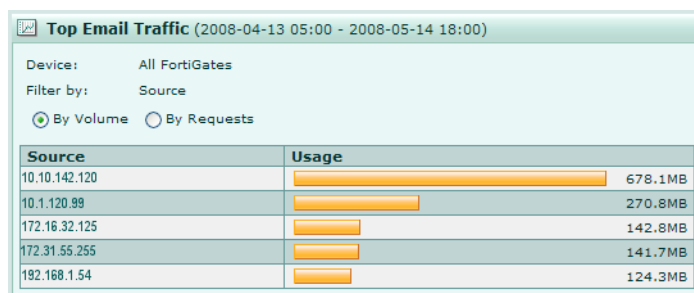
- 1 Go to **System > Dashboard**.
- 2 In Top FTP Traffic, select Edit in the title bar area.
- 3 Enter the appropriate information for the following:
 - Device** Select the registered device or device group from the drop-down list.
 - Display by** Select one of the following to filter the information:
 - Top Sources (to any) – filters only the top sources
 - Top Destinations (from any) – filters only the top destinations
 - Top Source and Destination (unique) – filters the top sources to unique destinations
 - Time Scope** Select one of the following for the time range:
 - Hour – filters the time by hour
 - Day – filters the time by the current day
 - Week – filters the time by the current week
 - Month – filters the time by the current month
 - No. Entries** Select the number of entries to display. For example, if you want to display 10 entries, select 10 from the drop-down list. You can specify only 5, 10, or 20.
- 4 Select OK.

Top Email Traffic

Top Email Traffic displays the total amount of email traffic happening on the FortiGate units. Top Email Traffic (By Volume) uses traffic logs to determine the total amount of email traffic and Top Email Traffic (By Request) uses content logs to determine the total amount of email requests. This information is displayed using a bar chart.

You can edit Top Email Traffic to customize the information that displays. The following procedure describes how to edit the Top Email Traffic widget.

Figure 17: Top Email Traffic widget



To edit the information for Top Email Traffic

- 1 Go to **System > Dashboard**.
- 2 In Top Email Traffic, select Edit.

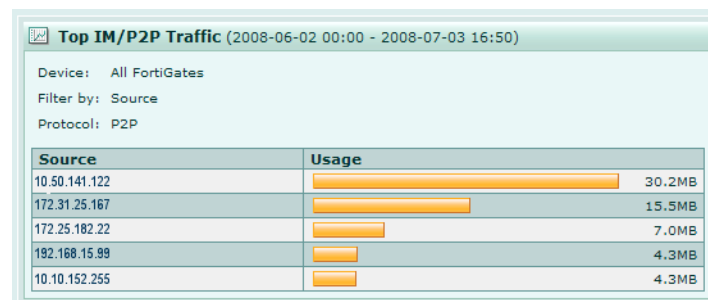
- 3 Enter the appropriate information for the following:
 - Device** Select the registered device or device group from the drop-down list.
 - Display by** Select one of the following to filter the information:
 - Top Sources (to any) – filters only the top sources
 - Top Destinations (from any) – filters only the top destinations
 - Top Source and Destination (unique) – filters the top sources to unique destinations
 - Filter Protocol** Select one of the following to filter by email protocol:
 - POP3
 - IMAP
 - SMTP
 - Filter Domain** Enter the domain name for filtering the information, for example the email server, mail.example.com
 - Time Scope** Select one of the following for the time range:
 - Hour – filters the time by hour
 - Day – filters the time by the current day
 - Week – filters the time by the current week
 - Month – filters the time by the current month
 - No. Entries** Select the number of entries to display. For example, if you want to display 10 entries, select 10 from the drop-down list. You can specify only 5, 10, or 20.
- 4 Select OK.

Top IM/P2P Traffic

Top IM/P2P Traffic displays the top instant messaging and P2P programs used, using a bar chart. The information displays each IM and P2P program separately by user. IM programs used display the top number of messages sent or received and P2P programs used display the top bandwidth of files sent or received.

You can edit Top IM/P2P Traffic to customize the information that displays. The following procedure describes how to edit the Top IM/P2P Traffic widget.

Figure 18: Top IM/P2P Traffic widget



To edit information for Top IM/P2P Traffic

- 1 Go to **System > Dashboard**.
- 2 In Top IM/P2P Traffic, select Edit in the title bar area.

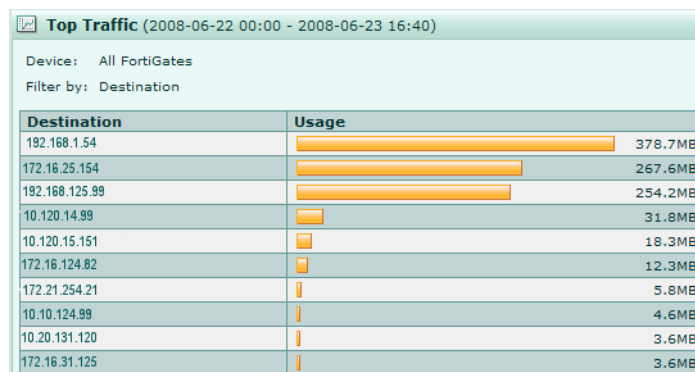
- 3 Enter the appropriate information for the following:
 - Type** Select the type of program you want displayed, either IM or P2P.
 - Device** Select the registered device or device group from the drop-down list.
 - Display by** Select one of the following to filter the information:
 - Top Sources (to any) – filters only the top sources
 - Top Destinations (from any) – filters only the top destinations
 - Top Source and Destination (unique) – filters the top sources to unique destinations
 - Protocol** Select the protocol
 - Time Scope** Select one of the following for the time range:
 - Hour – filters the time by hour
 - Day – filters the time by the current day
 - Week – filters the time by the current week
 - Month – filters the time by the current month
 - No. Entries** Select the number of entries to display. For example, if you want to display 10 entries, select 10 from the drop-down list. You can specify only 5, 10, or 20.
- 4 Select OK.

Top Traffic

Top Traffic displays the total amount of traffic for FortiGate units. Top Traffic uses traffic logs in determining the total amount of traffic. This information displays as a bar chart and only displays by volume.

You can edit Top Traffic to customize the information that displays. The following procedure describes how to edit the Top Traffic widget.

Figure 19: Top Traffic widget



To edit information for Top Traffic

- 1 Go to **System > Dashboard**.
- 2 In Top Traffic, select Edit in the title bar area.

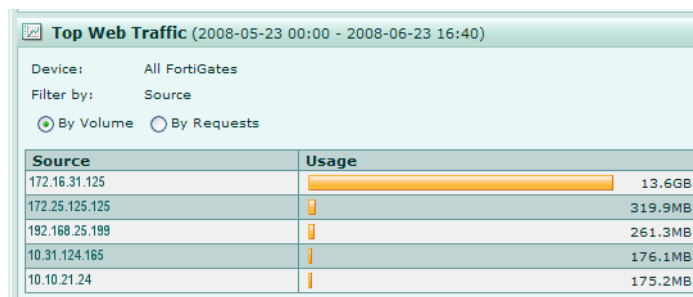
- 3 Enter the appropriate information for the following:
 - Device** Select the registered device or device group from the drop-down list.
 - Display by** Select one of the following to filter the information:
 - Top Sources (to any) – filters only the top sources
 - Top Destinations (from any) – filters only the top destinations
 - Top Source and Destination (unique) – filters the top sources to unique destinations
 - Filter Port** Select the type of port, TCP or UDP, and then enter the port number. The port number can be from 1 - 65535.
 - Time Scope** Select one of the following for the time range:
 - Hour – filters the time by hour
 - Day – filters the time by the current day
 - Week – filters the time by the current week
 - Month – filters the time by the current month
 - No. Entries** Select the number of entries to display. For example, if you want to display 10 entries, select 10 from the drop-down list. You can specify only 5, 10, or 20.
- 4 Select OK.

Top Web Traffic

Top Web Traffic displays the total web traffic usage on the network. This information is displayed as a bar chart. Information for this widget is gathered from the Web Filter logs, if you selected By Requests, or, if you selected By Volume, from the traffic logs.

You can edit Top Web Traffic to customize the information displayed. The following procedure describes how to edit the Top Web Traffic widget.

Figure 20: Top Web Traffic widget



To edit information for Top Web Traffic

- 1 Go to **System > Dashboard**.
- 2 In Top Web Traffic, select Edit.

- 3 Enter the appropriate information for the following:
 - Device** Select the registered device or device group from the drop-down list.
 - Display by** Select one of the following to filter the information:
 - Top Sources (to any) – filters only the top sources
 - Top Destinations (from any) – filters only the top destinations
 - Top Source and Destination (unique) – filters the top sources to unique destinations
 - Filter Source IP Address** Enter the source IP address.
 - Filter Destination IP Address** Enter the destination IP address.
 - Time Scope** Select one of the following for the time range:
 - Hour – filters the time by hour
 - Day – filters the time by the current day
 - Week – filters the time by the current week
 - Month – filters the time by the current month
 - No. Entries** Select the number of entries to display. For example, if you want to display 10 entries, select 10 from the drop-down list. You can specify only 5, 10, or 20.
- 4 Select OK.

Network

Use the network settings to configure the FortiAnalyzer unit to operate in your network. Basic network settings include configuring interfaces, DNS settings and static routes.

Interface

You can configure the interfaces on the FortiAnalyzer unit, including their IP address, and permitted remote administration protocols.

Figure 21: Interface list

Name	IP / Netmask	Access	FDP	Status	Modify
port1	172.20.120.139 / 255.255.255.0	HTTPS,PING,SSH,HTTP,TELNET,AGGREGATOR,WEBSERVICE	✔	Bring Down	
port2	192.168.2.99 / 255.255.255.0	HTTPS,PING,SSH,HTTP		Bring Down	
port3	192.168.3.99 / 255.255.255.0	HTTPS,PING,SSH,HTTP		Bring Down	
port4	192.168.4.99 / 255.255.255.0	HTTPS,PING,SSH,HTTP		Bring Down	

- Name** The name of the network interface on the FortiAnalyzer unit.
- IP/Netmask** The IP address and network mask configured for the interface.
- Access** A list of the administrative access methods available on the interface. For more information, see [“Administrative Access” on page 46](#).
- FDP** Fortinet Discovery Protocol (FDP) indicator. When Fortinet Discovery Protocol is enabled for an interface, a green check appears. For more information about FDP, see [“About Fortinet Discovery Protocol” on page 47](#) and [“Manually adding a FortiGate unit using the Fortinet Discovery Protocol \(FDP\)” on page 85](#).

Status	The status of the network interface. <ul style="list-style-type: none"> • A green arrow indicates the interface is up. Select Bring Down to disable the port. • A red arrow indicates the interface is down. Select Bring up to enable the port.
Modify	Select Modify to change the interface settings.

Changing interface settings

To change the interface settings

- 1 Go to **System > Network > Interface**.
- 2 In the row corresponding to the interface you want to change, select Modify.
- 3 Configure the following options:

Interface Name	The interface name is cannot be changed.
Fortinet Discovery Protocol	Select Enabled to allow responses to Fortinet Discovery Protocol (FDP) on the interface, allowing FortiGate devices to find the FortiAnalyzer unit automatically. For more information about FDP, see “About Fortinet Discovery Protocol” on page 47 and “Manually adding a FortiGate unit using the Fortinet Discovery Protocol (FDP)” on page 85 .
IP/Netmask	Enter an IP address and network mask.
Administrative Access	Select which methods of administrative access should be available on this interface. <ul style="list-style-type: none"> • HTTPS allows secure HTTPS connections to the FortiAnalyzer web-based manager. • PING allows response to ICMP pings, which are useful for testing connectivity. • HTTP allows HTTP connections to the FortiAnalyzer web-based manager. HTTP connections are <i>not</i> secure and can be intercepted by a third party. • SSH allows SSH connections to the FortiAnalyzer CLI. • TELNET allows Telnet connections to the FortiAnalyzer CLI. Telnet connections are <i>not</i> secure, and can be intercepted by a third party. • AGGREGATOR assigns the port to be the sender or receiver of log aggregation transmissions. For more information about aggregation, see “Configuring log aggregation” on page 58. • WEBSERVICES allows web service (SOAP) connections. FortiManagerunits require web service connections for remote management of FortiAnalyzer units. If this option is not enabled, the FortiManager unit will not be able to install a configuration on the FortiAnalyzer unit.

- 4 Select OK.

About Fortinet Discovery Protocol

FortiGate units running FortiOS version 3.0 or greater can use Fortinet Discovery Protocol (FDP), a UDP protocol, to locate a FortiAnalyzer unit.

When a FortiGate administrator selects Automatic Discovery, the FortiGate unit attempts to locate FortiAnalyzer units on the network within the same subnet. If FDP has been enabled for its interface to that subnet, the FortiAnalyzer unit will respond. Once the FortiGate unit discovers a FortiAnalyzer unit, the FortiGate unit automatically enables logging to the FortiAnalyzer and begins sending log data.

Depending on its configuration, the FortiAnalyzer unit may then automatically register the device and save its data, add the device but ignore its data, or ignore the device entirely. For more information, see [“Configuring unregistered device connection attempt handling” on page 79](#).

DNS

Configure primary and secondary DNS servers to provide name resolution required by FortiAnalyzer features such as NFS shares.



Note: Configure and verify your DNS settings. Incorrect DNS settings can cause other features.

To configure DNS settings

- 1 Go to **System > Network > DNS**.
- 2 Enter an IP address for a primary and secondary DNS server.

Primary DNS Server Enter the primary DNS server IP address.

Secondary DNS Server Enter a secondary DNS server IP address.

- 3 Select Apply.

Routing

The route list displays the static routes on the FortiAnalyzer unit.

To view the routing list, go to **System > Network > Routing**.

Figure 22: Route list

Create New				
#	Destination IP / Netmask	Gateway	Interface	Modify
1	0.0.0.0 / 0.0.0.0	192.168.1.1	port1	

- Destination IP/Netmask** The destination IP address and netmask of packets that the FortiAnalyzer unit wants to send to.
- Gateway** The IP address of the router where the FortiAnalyzer unit forwards packets.
- Interface** The names of the FortiAnalyzer interfaces through which intercepted packets are received and sent.
- Modify** Select to change the route configuration.
- Create New** Add a route to the route list.

Adding a route

Static routes provide the FortiAnalyzer unit with the information it needs to forward a packet to a particular destination other than the default gateway.

To add a static route

- 1 Go to **System > Network > Routing**.
- 2 Select Create New.
- 3 Configure the following options:

Destination IP Enter the destination IP address network mask of packets that the FortiAnalyzer unit has to intercept.

Mask Enter a netmask to associate with the IP address.

Gateway Enter the IP address of the gateway where the FortiAnalyzer unit will forward intercepted packets.

Interface Select a port from the list of available ports.

- 4 Select OK.

Admin

Use the Admin option to configure and maintain FortiAnalyzer administrators, administrative domains (ADOMs), set a user's administrative access and maintain passwords.

When the FortiAnalyzer unit is initially installed, it is configured with a single master administrator account with the user name of "admin". From this account, you can add and edit administrator accounts, control the access level of each administrator account and control the IP address for connecting to the FortiAnalyzer unit. This account is permanent, and cannot be deleted from the FortiAnalyzer unit.

When configuring administrators, you can add '@' symbol in the name. For example, admin_1@headquarters, to identify an administrator that will access the FortiAnalyzer unit from the headquarters office of their organization.

To view a list of administrators for the FortiAnalyzer unit, go to **System > Admin > Administrators**.

Figure 23: Administrator account list

Create New		Delete					
<input type="checkbox"/>	Name	Trusted Hosts	Profile	Type			
<input type="checkbox"/>	admin	0.0.0.0 / 0.0.0.0, 0.0.0.0 / 0.0.0.0, 127.0.0.1 / 255.255.255.255	prof_admin	Local			
<input type="checkbox"/>	tadmin	172.20.120.0 / 255.255.255.0, 0.0.0.0 / 0.0.0.0, 127.0.0.1 / 255.255.255.255	prof_read_only	Local			
<input type="checkbox"/>	tadmin2	0.0.0.0 / 0.0.0.0, 0.0.0.0 / 0.0.0.0, 127.0.0.1 / 255.255.255.255	taccessprofile	Local			

Delete
 Edit
 Change Password

Name	The assigned name for the administrator.
Trusted Hosts	The IP address and netmask of acceptable locations for the administrator to log in to the FortiAnalyzer unit. If you want the administrator to be able to access the FortiAnalyzer unit from any address, use the IP address and netmask 0.0.0.0/0.0.0.0. To limit the administrator to only access the FortiAnalyzer unit from a specific network or host, enter that network's IP and netmask.
Profile	The access profile assigned to the administrator.
Type	Type can be either local, as a configured administrator on the FortiAnalyzer unit or RADIUS if you are using a RADIUS server on your network.
Delete	Select to remove the administrator account. You cannot delete the account named <code>admin</code> .
Edit	Select to modify the account information.
Change Password	Select to change the account password. For more information, see "Changing an administrator's password" on page 50 .

Adding or editing an administrator account

You can add, edit or delete a FortiAnalyzer administrator account, except the default administrator `admin` administrator account.

When configuring the administrator's information, you can add the @ symbol to the administrator's name. For example, `jb@headquarters`. The @ symbol is also useful to those administrators who require RADIUS authentication.

To add or edit an administrator account

- 1 Go to **System > Admin > Administrators**.
- 2 Select Create New.
- 3 Configure the following options and select OK.

Administrator	Enter the administrator name. You can now add the @ symbol, if required.
Remote Auth	Select if you are using a RADIUS server group on your network.
Auth Group	Select which RADIUS server group to use when authenticating this administrator account. This option only appears if Remote Auth is enabled.
Password	Enter a password. For security reasons, a password should be a mixture of letters and numbers and longer than six characters. If a user attempts to log in and mis-types the password three times, the user is locked out of the system from that IP address for a short period of time. This does not appear when editing the account.
Confirm Password	Re-enter the password to confirm its spelling. This does not appear when editing the account.
Trusted Host	Enter the IP address and netmask of acceptable locations for the administrator to log in to the FortiAnalyzer unit. If you want the administrator to be able to access the FortiAnalyzer unit from any address, use the IP address and netmask 0.0.0.0/0.0.0.0. To limit the administrator to only access the FortiAnalyzer unit from a specific network, enter that network's IP and netmask.

Access Profile	Select an access profile from the list. Access profiles define administrative access permissions to areas of the configuration by menu item. For more information, see “Access Profile” on page 50 .
Admin Domain	Select an administrative domain (ADOM) from the list. ADOMs define administrative access permissions to areas of the configuration and device data by device or VDOM. For more information, see “Administrative Domains (ADOMs)” on page 19 . This option does not appear when ADOMs are disabled, or for the <code>admin</code> administrator.

Changing an administrator’s password

The `admin` administrator and administrators with read and write permissions can change their own account passwords.

Administrators with read-only permissions cannot change their own password. Instead, the `admin` administrator must change the password for them.

To change the administrator account password

- 1 Go to **System > Admin > Administrators**.
- 2 Select the Change Password icon.
- 3 Enter the old password for confirmation.
- 4 Enter the new password and confirm the spelling by entering it again.
- 5 Select OK.

Access Profile

Only the `admin` administrator has access to all configuration areas of a FortiAnalyzer unit by default. Every other administrator must be assigned an access profile.

Access profiles define administrator privileges to parts of the FortiAnalyzer configuration. For example, you can have a profile where the administrator only has read and write access to the reports, or assign read-only access to the content archive logs.

You can create any number of access profiles. For each profile, you can define what access privileges are granted. Administrator accounts can only use one access profile at a time.

Figure 24: Access Profile

New Access Profile

Profile Name:

Access Control	<input type="checkbox"/> None	<input type="checkbox"/> Read Only	<input type="checkbox"/> Read-Write
Network	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Admin	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
System	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
IP Alias	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Devices	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Alerts	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Network Summary	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Forensic	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Content Archive	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Report	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Logs	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Quarantine	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Network Analyzer	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Vulnerability Scan	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Admin Domains	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>



Note: Administrator accounts can also be restricted to specific devices or VDOMs in the FortiAnalyzer device list. For more information, see [“Administrative Domains \(ADOMs\)”](#) on page 19.

To create an access profile

- 1 Go to **System > Admin > Access Profile**.
- 2 Select Create New.
- 3 Enter a name for the profile.
- 4 Select a filter for each option:

None	The administrator has no access to the function.
Read Only	The administrator can view pages, menus and information, but cannot modify any settings.
Read-Write	The administrator can view pages, menus and information as well as change configurations.

Auth Group

Auth Group enables you to group RADIUS servers in to logical arrangements for administrator authentication.

You must first configure at least one RADIUS server before you can create an authorization group.

To add a group

- 1 Go to **System > Admin > Auth Group**.
- 2 Select Create New.
- 3 Select the servers from Available Auth Servers to add to the group and select the right arrow.
- 4 Select OK.

RADIUS Server

RADIUS servers authenticate administrators. The following procedure explains how to add a RADIUS server for authenticating administrators.

To add a RADIUS server

- 1 Go to **System > Admin > RADIUS Server**.
- 2 Select Create New.
- 3 Configure the following and select OK:

Name	Enter a name to identify the server.
Server IP/Name	Enter the IP address for the server.
Shared Secret	Enter the password for the server.
Authentication Protocol	Select which protocol the FortiAnalyzer unit will use to communicate with the RADIUS server.

Administrator Settings

Administrators Settings enables you to configure some common settings for all administrator accounts, including the idle timeout (how much time must pass without activity before the FortiAnalyzer unit logs out an administrator), the language for the web-based manager, and the PIN for the LCD panel. You can also enable or disable administrative domains (ADOMs).

To configure administrators, go to **System > Admin**.



Note: Only the `admin` administrator can add or change administrator account information.

Figure 25: Administrators Settings

Idle Timeout Set the idle timeout to control the amount of inactive time before the administrator must log in again. To improve security keep the idle timeout to a low value (for example, five minutes). Note that sessions will not time out when viewing real-time logs.

Web Administration Language Set the language for the web-based manager.

PIN Protection	Enable then enter a Personal Identification Number (PIN) to secure the LCD access to FortiAnalyzer units with an LCD panel. The PIN must be six numbers. This option only appears on models with an LCD panel.
Admin Domain Configuration	Enable or disable administrative domains (ADOMs). For more information on ADOMs, see “Administrative Domains (ADOMs)” on page 19 . This option does not appear if ADOMs are currently enabled and ADOMs other than the <code>root</code> ADOM exist. This option does not appear on FortiAnalyzer-100 or FortiAnalyzer-100A/100B models.

Monitor

The Monitor page enables the `admin` administrator to view other administrators currently logged in to the FortiAnalyzer unit. The `admin` administrator can disconnect other administrators, should the need arise.

To monitor current administrators, go to **System > Admin > Monitor**.

To disconnect an administrator, select a check box next to the administrator's user name and select Disconnect.

Network Sharing

The FortiAnalyzer hard disk can be used as an NFS or Windows network share to store and share user files, as well as sharing FortiAnalyzer reports and logs.

Use Network Sharing to configure network share users and access.

When selecting a network share style, consider the access methods available to your users:

- Microsoft Windows users could connect to a FortiAnalyzer Windows network share by mapping a drive letter to a network folder
- Apple Mac OS X, Unix or Linux users:
 - could mount a FortiAnalyzer Windows network share using `smbfs`
 - could mount a FortiAnalyzer NFS network share

Before a user can access files on the FortiAnalyzer network share:

- network share user accounts and groups must be created
- network sharing (Windows or NFS) must be enabled
- the share folder and its file permissions (user access) must be set

Adding share users

You can create network share user accounts to provide non-administrative access to the log, reports and hard disk storage of the FortiAnalyzer unit.

Users added will not have administrative access to the FortiAnalyzer hard disk or FortiAnalyzer unit. To add administrative users, see [“Admin” on page 48](#).

To add a user account

- 1 Go to **System > Network Sharing > User**.
- 2 Select Create New.

- 3 Enter the following information for the user account and select OK:
 - User name** Enter a user name.
The name cannot include spaces.
 - UID (NFS only)** Enter a user ID.
Use this field only if you are using NFS shares. The NFS protocol uses the UID to determine the permissions on files and folders.
 - Password** Enter a password for the user.
 - Description** Enter a description of the user. For example, you might enter the users name or a position such as IT Manager.

Adding share groups

You can create network share user groups to maintain access privileges for a large number of users at once.

To add a user group

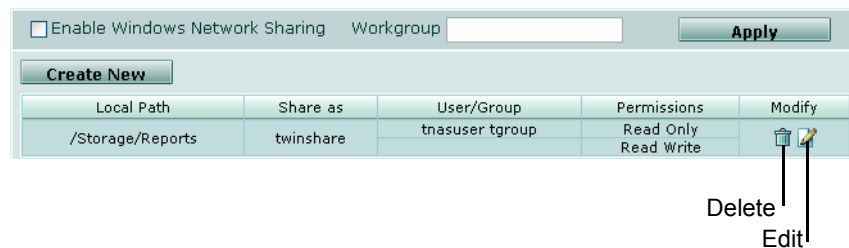
- 1 Go to **System > Network Sharing > Group**.
- 2 Select Create New.
- 3 Enter the following information for the group account:
 - Group** Enter a user name. For example, `Finance`. The name cannot include spaces.
 - GID (NFS only)** Enter a Group ID. Use this field if you are using NFS shares. The NFS protocol uses the GID to determine the permissions on files and folders.
- 4 Select the users from the Available Users area and select the Right arrow to add them to the group.
To remove a user, select a user from the Members area and select the Left arrow.
- 5 Select OK.

Configuring Windows shares

You can configure the FortiAnalyzer unit to provide folder and file sharing using Windows sharing.

To view users with Windows share access to the FortiAnalyzer unit, go to **System > Network Sharing > Windows Share**.

Figure 26: Windows network shares



- Local Path** The shared file or folder path.
- Share as** The share name.
- User/Group** A list of users or groups that have access to the folder or files.

Permissions	Permissions for the user or groups. This can be either Read Only or Read Write.
Modify	Select Edit to change any of the options for file sharing. Select Delete to remove the file share.

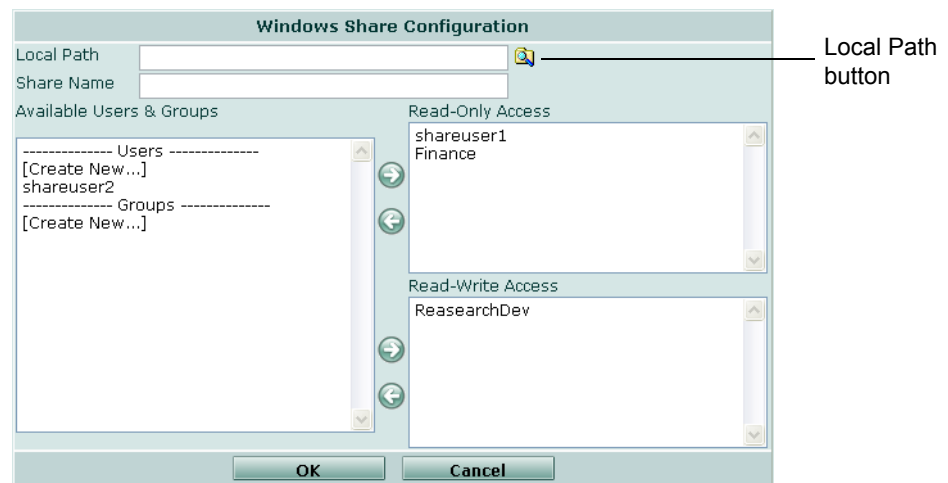
To enable Windows shares

- 1 Go to **System > Network Sharing > Windows Share**.
- 2 Select Enable Windows Network Sharing.
- 3 Enter a Workgroup name.
- 4 Select Apply.
- 5 Configure a share folder and user permissions to access that share. For more information, see [“Assigning user permissions” on page 55](#).

Assigning user permissions

After configuring users and user groups, configure the files and folders the users can access, and their Windows share read/write access privileges.

Figure 27: Windows share configuration



To add a new Windows share configuration

- 1 Go to **System > Network Sharing > Windows Share**.
- 2 Select Create New.
- 3 Select the Local Path button to define which folder on the FortiAnalyzer unit hard disk to share.



Note: The default permissions for files and folders is read and execute privileges. The owner of the document also has write privileges. You must select the write permission for the folder, user and the group to enable write permissions. For more information, see [“Default file permissions on NFS shares” on page 56](#).

- 4 Select OK.
- 5 Enter the Share Name to describe the shared folder.
- 6 Select user and group names from the Available Users & Groups box. Hold the Ctrl key to select multiple users or groups.





- 7 Select the type of access rights the users and groups will have and select the appropriate right arrow to move the user or group name to the Read-Only Access or Read-Write Access boxes.
- 8 Select Ok.



Configuring NFS shares

You can configure the FortiAnalyzer unit to provide folder and file sharing using NFS sharing.

To view a list of users with NFS share access to the FortiAnalyzer unit, including access privileges, go to **System > Network Sharing > NFS Export**.

Figure 28: NFS shares

Local Path	Remote Clients	Permissions	Modify
/Storage/Reports/FortiGate	10.10.10.1	Read Only Read Write	 
/Storage/reports/FortiGate/.sample/Content_Activity	10.20.10.2	Read Only Read Write	 

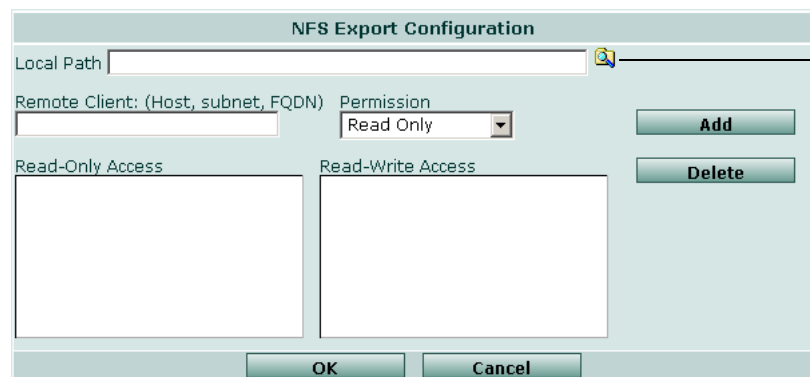
 Edit
 Delete

Local Path	The path the user has permission to connect to.
Remote Clients	A list of users that have access to the folder or files.
Permissions	Permissions for the user. This can be either Read Only or Read Write.
Modify	Select Edit to change any of the options for file sharing. Select Delete to remove the file sharing permissions.

To add a new NFS share configuration

- 1 Go to **System > Network Sharing > NFS Export**.
- 2 Select Enable NFS Exports and select Apply.
- 3 Select Create New.

Figure 29: NFS share configuration



The dialog box titled "NFS Export Configuration" contains the following fields and controls:

- Local Path:** A text input field with a search icon (magnifying glass) to its right, labeled "Local Path button".
- Remote Client:** A text input field with the placeholder "(Host, subnet, FQDN)".
- Permission:** A dropdown menu currently set to "Read Only".
- Buttons:** "Add" and "Delete" buttons are located to the right of the Remote Client and Permission fields.
- Read-Only Access:** An empty list box for users with read-only permissions.
- Read-Write Access:** An empty list box for users with read-write permissions.
- Footer:** "OK" and "Cancel" buttons.

- 4 Select the Local Path button to define which folder on the FortiAnalyzer unit hard disk to share.



Note: The default permissions for files and folders is read and execute privileges. The owner of the document also has write privileges. To enable write access for users and groups, you must select the write permission for the folder and for the user and the group. For more information, see [“Default file permissions on NFS shares” on page 56](#).

- 5 Select OK.
- 6 In Remote Clients, enter the IP address or domain name of the remote system or user ID.
- 7 Select the type of Permission required and select Add.
- 8 Select OK.

Default file permissions on NFS shares

By default, when a user adds a new file or folder, the permissions are:

- read, write, execute for the owner (user)
- read and execute for the Admin group and Others group.

You can set file permissions in the CLI. For more information, see the `config nas share` command in the [FortiAnalyzer CLI Reference](#).

Config

You can use **System > Config** to setup and maintain miscellaneous features, such as local logging, log aggregation, log forwarding, IP aliases, and LDAP connections.

Automatic file deletion and local log settings

The FortiAnalyzer unit creates its own system log messages to provide information on system events occurring on the unit, such as system activity, administration events and IPSec negotiations with configured devices.

To configure logging behavior for your FortiAnalyzer unit, go to **System > Config > Log Setting**.

Figure 30: FortiAnalyzer unit log settings

Log Settings

Log Locally

Log Level: ▾

Allocated Disk Space (MB) / 9 used / 102958 available

Log options when disk is full Overwrite Oldest Files Stop Logging

Use System Device Log Settings

Log to Host

IP: Port:

Log Level: ▾ Format: CSV format

▼ **Event Log**

Event Type	<input checked="" type="checkbox"/> Log Locally	<input type="checkbox"/> Log to Host
When configuration has changed	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IPSec negotiation event	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Admin login/logout event	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
System activity event	<input checked="" type="checkbox"/>	<input type="checkbox"/>

▼ **Automatically Delete**

Logs older than Months ▾

Network analyzer logs older than Months ▾

Local logs older than Months ▾

Reports older than Months ▾

Apply

- Log Locally** Select to save the FortiAnalyzer log messages on the FortiAnalyzer hard disk.
- Log Level** Select the severity level for the log messages recorded to the FortiAnalyzer hard disk. The FortiAnalyzer unit logs all levels of severity down to, but not less severe than, the level you select. For example, if you want to record emergency, critical, and error messages, select Error.
- Allocated Disk Space (MB)** The maximum size of the FortiAnalyzer log file that the FortiAnalyzer unit saves to the hard disk.
When the log file reaches the specified maximum size, the FortiAnalyzer unit saves current network traffic log file with an incremental number and starts a new active log file.
- Log options when log disk is full** The policy to follow for saving the current log and starting a new active log when the FortiAnalyzer disk is full.
Select Overwrite Oldest Files to delete the oldest log entry when the disk is full.
Select Stop Logging to stop logging messages when the disk is full.
- Use System Device Log Settings** Enable to use the same settings for local FortiAnalyzer logs as device logs. For information about device log settings, see [“Rolling and uploading logs” on page 104](#).
- Log file should not exceed** Enter the maximum size of the current log file that the FortiAnalyzer unit will save to the hard disk. When the log file reaches the specified maximum size, the FortiAnalyzer unit saves the current log file and starts a new active log file.
When a log file reaches its maximum size, the FortiAnalyzer unit saves the log files with an incremental number, and starts a new log file with the same name.
This option appears only when Use System Device Log Settings is disabled.

Log file should be rolled... even if size is not exceeded	<p>Select the frequency of when the FortiAnalyzer unit renames the current log file and starts a new active log file.</p> <ul style="list-style-type: none"> • Daily: Roll log files daily, even if the log file has not yet reached maximum file size. • Weekly: Roll log files weekly, even if the log file has not yet reached maximum file size. • Optional: Roll log files only when the log file reaches the maximum file size, regardless of time interval. <p>This option appears only when Use System Device Log Settings is disabled.</p>
Log to Host	Select to send log messages generated by the FortiAnalyzer unit to another host, such as a Syslog server.
IP	Enter the IP address of the Syslog server.
Port	Enter the Syslog port. The default port is 514.
Log Level	Select the severity level for the log messages recorded to the Syslog server. The FortiAnalyzer unit logs all levels of severity down to, but not less severe than, the level you select. For example, if you want to record emergency, critical, and error messages, select Error.
Format	Enable CSV format to record log messages in comma-separated value (CSV) formatted files. Log message fields are separated by commas. When disabled, logs are recorded as standard log files.
Event Log	Select to configure which FortiAnalyzer unit events the FortiAnalyzer unit records to the log. Events can be logged locally on the FortiAnalyzer unit, or to the host indicated in Log to Host. Loggable event types include When configuration has changed, IPSec negotiation event, Admin login/logout event, and System activity event.
Automatically Delete	Select to configure automatic deletion of older logs. Enable the type of log or report you wish to automatically delete (Logs older than, Network analyzer logs older than, Local logs older than, Reports older than, Content archive files older than), then select from Hours, Weeks, Days or Months, and enter the value for the age unit.

Configuring log aggregation

Log aggregation is a method of collecting log data from one or more FortiAnalyzer units to a central FortiAnalyzer unit.

Log aggregation involves one or more FortiAnalyzer units configured to act as aggregation clients, and a FortiAnalyzer unit configured to act as an aggregation server. The aggregation client sends all of its device logs, including quarantined or content archived files, to the aggregation server. The transfer includes the active log to the point of aggregation (for example, `tlog.log`) and all rolled logs stored on the aggregation client (`tlog.1.log`, `tlog.2.log`, `tlog.3.log` ...). Subsequent log aggregations include only changes; the aggregation client does not re-send previously aggregated logs.

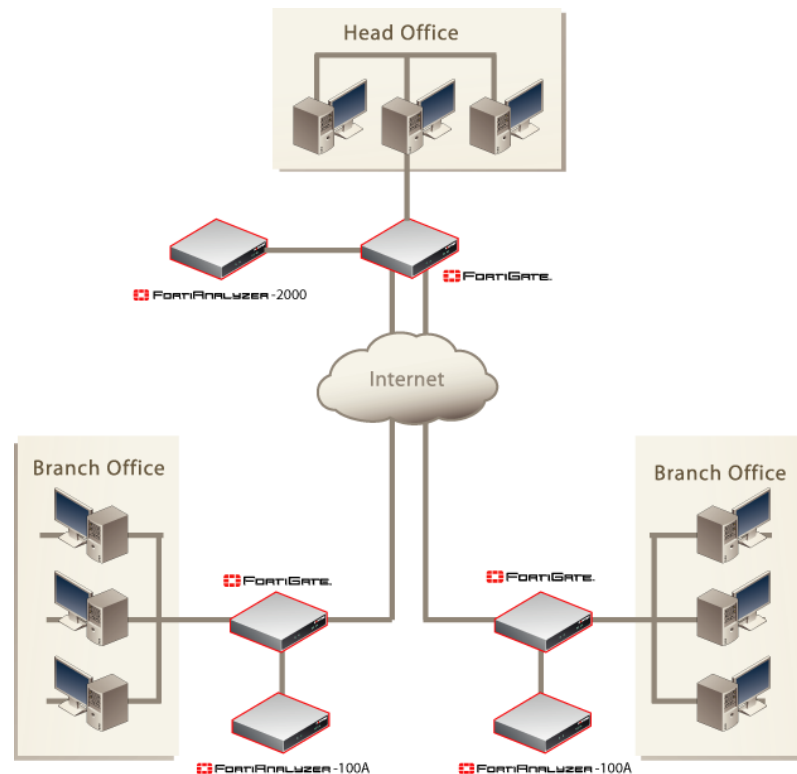
On the aggregation server, additional devices will appear in the device list, corresponding to those devices which log to the aggregation clients. You can easily identify these devices, as they do not have Rx and Tx permissions.

For example, a company may have a headquarters and a number of branch offices. Each branch office has a FortiGate unit and a FortiAnalyzer-100A/100B to collect local log information. Those branch office FortiAnalyzer units are configured as log aggregation clients. The headquarters has a FortiAnalyzer-2000/2000A which is configured as a log aggregator. The log aggregator collects logs from each of the branch office log aggregation clients, enabling headquarters to run reports that reflect all offices.



Note: For more information about log aggregation port numbers, see the Knowledge Center article [Traffic Types and TCP/UDP Ports used by Fortinet Products](#).

Figure 31: Example log aggregation topology



All FortiAnalyzer models can be configured as a log aggregation client, but log aggregation server support varies by FortiAnalyzer model, due to storage and resource requirements.

FortiAnalyzer Model	Aggregation Client	Aggregation Server
FortiAnalyzer-100A/100B	Yes	No
FortiAnalyzer-400	Yes	No
FortiAnalyzer-800/800B	Yes	Yes
FortiAnalyzer-2000/2000A	Yes	Yes
FortiAnalyzer-4000/4000A	Yes	Yes

Configuring an aggregation client

An aggregation client is a FortiAnalyzer unit that sends logs to a aggregation server. These include models such as the FortiAnalyzer-100A/100B and FortiAnalyzer-400.

To configure the aggregation client

- 1 Go to **System > Config > Log Aggregation**.
- 2 Select Enable log aggregation TO remote FortiAnalyzer.
- 3 Set the following settings and select OK:

Remote FortiAnalyzer IP	Enter the IP address of the FortiAnalyzer unit acting as the aggregation server.
Password	Enter the password for the aggregation server.
Confirm Password	Enter the password again for the aggregation server.
Aggregation daily at	Select the time of the day when the aggregation client uploads the logs to the aggregation server.
Aggregate Now	Select to send the logs to the aggregation server immediately. Use this when you want to create a report on the server with the most current log data.

Configuring an aggregation server

An aggregation server is a FortiAnalyzer unit that receives the logs sent from an aggregation client. FortiAnalyzer-800/800B models and higher can be configured as aggregation servers.

To configure the aggregation server

- 1 Go to **System > Config > Log Aggregation**.
- 2 Select Enable log aggregation TO this FortiAnalyzer.
- 3 Set the following settings and select OK:

Password	Enter the password for the aggregation server.
Confirm Password	Enter the password again for the aggregation server.

Configuring log forwarding

Log forwarding sends duplicates of log messages received by the FortiAnalyzer unit to a separate Syslog server. This can be useful for additional log storage or processing.

The log forwarding destination (Remote device IP) may receive either a full duplicate or a subset of those log messages that are received by the FortiAnalyzer unit. Log messages are forwarded only if they meet or exceed the Minimum Severity threshold.

Log forwarding is similar to log uploading or log aggregation, but log forwards are sent as individual Syslog messages, not whole log files over FTP, SFTP, or SCP, and not as batches of log files.

To forward log events

- 1 Go to **System > Config > Log Forwarding**.
- 2 Select Enable log forwarding to remote log server.

- 3 Enter the IP address of the external syslog server in Remote device IP.
- 4 Select whether to Forward all incoming logs or Forward only authorized logs (authorized according to a device's permissions in the device list).
- 5 Select the Minimum Severity threshold.
All log events of equal or greater servers will be transmitted.
For example, if the selected Minimum Severity is Critical, all Emergency, Alert and Critical log events will be forwarded; other log events will not be forwarded.
- 6 Select Apply.

Configuring IP aliases

Use IP Alias to assign a meaningful name to IP addresses. When configuring reports, or viewing logs and content archives, select Resolve Host Name to view the alias rather than the IP address.

IP aliases can make logs and reports easier to read and interpret. For example, you could create an IP alias to display the label `mailserver1` instead of its IP address, `10.10.1.54`.

To add an IP alias

- 1 Go to **System > Config > IP Alias**.
- 2 Enter a nickname for the IP address in Alias.
- 3 Enter the IP address or range in Host(Subnet / IP Range).
- 4 Select Add.

To edit an IP alias

- 1 Go to **System > Config > IP Alias**.
- 2 In the Action column, select Edit.
- 3 Modify the nickname for the IP address in Alias.
- 4 Modify the IP address or range in Host(Subnet / IP Range).
- 5 Select Update Now.

Importing an IP alias list file

To create a large number of IP aliases as a single batch, you can import a text file containing this information.

The contents of the text file should be in the format:

```
<ip address> <alias_name>
```

For example:

```
10.10.10.1 User_1
```

There can be only one IP address/user name entry per line.

To import the alias file

- 1 Go to **System > Config > IP Alias**.
- 2 Select Import.

- 3 Enter the path and file name or select Browse to locate the file.
- 4 Select OK.

IP alias ranges

When adding an IP alias you can include an IP address range as well as individual addresses. For example:

- 10.10.10.1 - 10.10.10.50
- 10.10.10.1 - 10.10.20.100

Configuring RAID

FortiAnalyzer units containing multiple hard disks can store data using a RAID array to provide redundant storage, data protection, faster hard disk access, or a larger storage capacity.

RAID settings can be configured from the Dashboard, in the RAID Monitor widget as well as from **System > Config > RAID**.



Caution: Fortinet recommends using RAID 10 if your FortiAnalyzer unit uses software RAID and redundancy is required. Using RAID 5 causes system performance issues.



Note: RAID functionality is only available on the FortiAnalyzer-400, FortiAnalyzer-800/800B, FortiAnalyzer-2000/2000A and FortiAnalyzer-4000/4000A. These units include multiple hard disks for RAID support.

Array capacity is limited to 8 TB. This limit is included only in the following previous releases:

- FortiAnalyzer 3.0 MR6 patch release 1
- FortiAnalyzer 3.0 MR5 patch release 5

RAID levels

All FortiAnalyzer units support standard RAID levels 0, 1, 5 and 10. Other RAID support varies by model:

- FortiAnalyzer-100A/100B: none
- FortiAnalyzer-400: Linear, 0, 1, 5, 10 (RAID5 is configured in the CLI)
- FortiAnalyzer-800/800B: Linear, 0, 1, 5, 10 (RAID5 is configured in the CLI)
- FortiAnalyzer-2000/2000A: 0, 10 5, 50, 5 with hot spare
- FortiAnalyzer-4000/4000A: 0, 10 5, 50, 5 with hot spare

If a hard disk fails, and the selected RAID level cannot be accomplished using the number of remaining hard disks, the FortiAnalyzer unit rebuilds the RAID using the default RAID level. Default RAID level varies by model. By default, FortiAnalyzer models with hardware RAID controllers use RAID 5; models with software RAID controllers use RAID 10.

FortiAnalyzer units that contain software RAID are the FortiAnalyzer-400, FortiAnalyzer-800/800B units. Hardware RAID is found on higher-end models, such as FortiAnalyzer-2000/2000A, FortiAnalyzer-4000/4000A.

You can find out information about RAID from the `get system status` command or `diag raid info` in the CLI.



Note: Fortinet recommends having an Uninterruptible Power Supply (UPS) in the event of a power failure. UPS is recommended because when a power failure occurs, data in the write cache is lost. Write cache is used to store data locally in memory before being written to the disk drive media, and then continuing on to the next task.

Linear

A linear RAID level combines all hard disks into one large virtual disk. It is also known as concatenation or JBOD (Just a Bunch of Disks). The total space available in this option is the capacity of all disks used. There is very little performance changes when using this RAID format, including any redundancy available at this level. If any of the drives fails, the entire set of drives is unusable until the faulty drive is replaced. All data will be lost. Linear RAID is available on FortiAnalyzer-400 and FortiAnalyzer-800/800B units.

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 of the drives fail, the data cannot be recovered. This RAID level is beneficial because it provides better performance, since the FortiAnalyzer unit can distribute disk writing across multiple disks.

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 several backup hard disks available. With a FortiAnalyzer-400 for example, if one disk fails, there are still three other hard disks the FortiAnalyzer unit can access and continue functioning.

RAID 5

A RAID 5 array employs striping with a parity check. The FortiAnalyzer unit writes information evenly across all drives. 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, on a FortiAnalyzer-400 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 writing, although performance is degraded when one disk has failed or is missing. RAID 5 also ensures no data loss. If a drive fails, it can be replaced and the FortiAnalyzer unit will restore the data on the new disk using reference information from the parity volume.



Note: RAID 5 appears in the web-based manager only for FortiAnalyzer units with hardware RAID.

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. Any drive from a RAID 1 array can fail without 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.



Note: Fortinet recommends using RAID 10 for redundancy instead of RAID 5 on FortiAnalyzer units with software RAID. RAID 5 causes system performance issues.

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). RAID 50 provides increased performance and also ensures no data loss for the same reasons as RAID 5. For the following FortiAnalyzer units, data is recoverable when:

- up to three disks fail (FortiAnalyzer-4000/4000A)
- up to two disks fail (FortiAnalyzer-2000/2000A).

RAID 5 with hot spare

FortiAnalyzer-2000/2000A and FortiAnalyzer-4000/4000A units can use one of their hard disks as a hot spare (a stand-by disk for the RAID), should any of the other RAID hard disks fail. If a hard disk fails, within a minute of the failure, the FortiAnalyzer unit begins to automatically substitute the hot spare for the failed drive, integrating it into the RAID array, and rebuilding the RAID's data.

When you replace the failed hard disk, the FortiAnalyzer unit uses the new hard disk as the new hot spare.



Note: RAID 10 requires an even number of disks. For example, on the FortiAnalyzer-2000/2000A, when selecting RAID 10 with hot spare, the FortiAnalyzer unit will use four of the six disks in the RAID 10 array, keeping one as a hot spare. The additional hard disk will be defined as idle.

The FortiAnalyzer-2000/2000A and FortiAnalyzer-4000/4000A also supports hot swapping of hard drive disks during operation. For more information, see [“Hot swapping the FortiAnalyzer-2000/2000A and FortiAnalyzer-4000/4000A” on page 66](#).

Hot swapping hard disks

Hot swapping refers to removing a failed hard disk and replacing it with a new one while the FortiAnalyzer unit remains in operation.

FortiAnalyzer-100A/100B and FortiAnalyzer-100 units have a single hard disk. Hot swapping is not available on these models.

FortiAnalyzer-400 models and higher can hot swap hard disks. For more information, see the Knowledge Center article [Replacing Hard Disks on the FortiAnalyzer](#).

Hot swapping is supported only in FortiAnalyzer firmware 3.0 MR1 (build 292) and higher. Hard disks in FortiAnalyzer units running firmware 3.0 (build 219) or earlier are not hot swappable. Before replacing a disk, verify your firmware version in the Dashboard of the web-based manager.

You can use any brand of hard disk to replace a failed hard disk, as long as it has the same capacity or greater. For example, if replacing a 120 GB hard drive, you could use either a 120 GB or 250 GB hard drive.



Caution: Do not replace a failed RAID hard disk with a smaller capacity hard disk. Using a smaller capacity hard disk will reduce the RAID's total capacity, resulting in data loss when the RAID is reconfigured for its smallest drive.

Hot swapping in the FortiAnalyzer-400 and FortiAnalyzer-800/800B

The following diagram indicates the drive number and their location in the FortiAnalyzer unit when you are looking at the front of the unit. Refer to this diagram before removing the disk drive to ensure you remove the correct one.

Table 3: FortiAnalyzer-400 disk drive configuration.

Drive 1 (p1)
Drive 2 (p2)
Drive 3 (p3)
Drive 4 (p4)

Table 4: FortiAnalyzer-800/800B disk drive configuration.

Drive 1	Drive 2	Drive 3	Drive 4
---------	---------	---------	---------



Caution: Hot swapping is supported in RAID 1, 5, 10, 50, and 5 with hot spare.

To swap a FortiAnalyzer-400 or FortiAnalyzer-800/800B hard disk

- 1 Go to **System > Config > RAID**.

If you are using the RAID Monitor widget, select RAID Settings in the title bar area. The RAID Monitor widget displays a warning symbol next to the failed disk.

- 2 Select Remove for the failed hard disk.

A message displays indicating it is safe to remove the disk from the drive.

- 3 Remove the hard disk from the drive bay on the FortiAnalyzer unit
 - On the FortiAnalyzer-400, open the faceplate, remove the screws for the drive and pull out the drive.
 - On the FortiAnalyzer-800/800B, pull open the face plate, unlock the drive and pull out the drive.

- 4 Insert the new hard disk into the empty drive bay on the FortiAnalyzer unit, reversing the steps above.

- 5 Refresh the RAID page.

The FortiAnalyzer disk controller will scan the available hard disks and update its information with the new hard disk.

- 6 Select Add to add the hard disk to the RAID array.

The FortiAnalyzer unit rebuilds the RAID array with the new hard disk.

Hot swapping the FortiAnalyzer-2000/2000A and FortiAnalyzer-4000/4000A

The following diagram indicates the drive number and their location in the FortiAnalyzer unit when you are looking at the front of the unit. Refer to this diagram before removing the disk drive to ensure you remove the correct one.

You can use any brand of hard disk to replace a failed hard disk; however, you must ensure that the hard disk size is the same size or larger as the remaining working drives. Using a smaller drive will affect the RAID setup. The FortiAnalyzer unit will reconfigure the RAID for the smallest drive, potentially causing data loss.

Table 5: FortiAnalyzer-2000/2000A disk drive configuration

Drive 1 (p1)	Drive 4 (p4)
Drive 2 (p2)	Drive 5 (p5)
Drive 3 (p3)	Drive 6 (p6)

Table 6: FortiAnalyzer-4000 disk drive configuration

Drive 1 (p1)	Drive 4 (p4)	Drive 7 (p7)	Drive 10 (p10)
Drive 2 (p2)	Drive 5 (p5)	Drive 8 (p8)	Drive 11 (p11)
Drive 3 (p3)	Drive 6 (p6)	Drive 9 (p9)	Drive 12 (p12)

The FortiAnalyzer-4000A can have different disk drive configurations because the disk layout depends on the RAID controller model.

To swap a hard disk

1 Go to **System > Config > RAID.**

If you are using the RAID Monitor widget, select RAID Settings in the title bar area. The RAID Monitor widget displays which hard disk has failed, displaying a warning symbol next to the failed disk.

2 Select Remove for the failed hard disk.

3 Remove the hard disk from the drive bay on the FortiAnalyzer unit.

- On the FortiAnalyzer-2000/2000A, press in the tab and pull the drive handle to remove the drive.
- On the FortiAnalyzer-4000/4000A, using a screw driver, turn the handle lock so it is horizontal. Push the blue latch right and pull the drive handle to remove the drive.

4 Select Click to start the controller re-scan.

The FortiAnalyzer disk controller scans the available hard disks and updates the RAID array for the remaining hard disks. The RAID array status will be "Degraded".

5 Insert the new hard disk into the empty drive bay on the FortiAnalyzer unit.

6 Select Click to start controller re-scan.

The FortiAnalyzer disk controller will scan the available hard disks and update its information with the new hard disk.

7 Select Add to add the hard disk to the RAID array.

The FortiAnalyzer unit rebuilds the RAID array with the new hard disk.

The options available here will depend on the RAID level selected. For most RAID levels, you can only add the new hard disk back into the RAID array. If you are running a RAID level with hot spare, you can also add the new hard disk as the hot spare.

Configuring RAID on the FortiAnalyzer-400 and FortiAnalyzer-800/800B

The FortiAnalyzer-400 and FortiAnalyzer-800/800B have four hot swappable hard disks. Hot swapping is available when running the FortiAnalyzer unit with RAID level 1 and 5.

RAID settings can be configured from the Dashboard, in the RAID Monitor widget as well as from **System > Config > RAID**.

For more information about the different RAID levels, see [“RAID levels” on page 62](#).



Caution: Back up all data before changing the RAID level. If you change RAID levels, the FortiAnalyzer unit reformats the hard disks to support the new setting, which may result in data loss.

Figure 32: RAID settings

Disk #	Size	Status
1	465.76GB	OK
2	465.76GB	OK
3	465.76GB	OK
4	465.76GB	OK

RAID Level	Select a RAID level and select Apply.
Total Disk Space	The amount of disk space available within the RAID array. This value will change depending on the RAID type selected.
Free Disk Space	The amount of free disk space.
Disk #	The number identifying the disk.
Size	The total size of the unit for the RAID level or the size of the spare hard disk.
Status	The status of the hard disk. For example, when functioning normally, “OK” appears.
Apply	Select to apply a change to the settings.

Configuring RAID on the FortiAnalyzer-2000/2000A and FortiAnalyzer-4000/4000A

The FortiAnalyzer-2000/2000A has six hard disks and the FortiAnalyzer-4000/4000A has 12 hard disks. For both units, the disks are hot-swappable. This provides additional RAID options for greater flexibility for data recovery, should a hard disk fail.

RAID settings can be configured from the Dashboard, in the RAID Monitor widget as well as from **System > Config > RAID**.



Caution: Back up all data before changing the RAID level. If you change RAID levels, the FortiAnalyzer unit reformats the hard disks to support the new setting, which may result in data loss.

Figure 33: FortiAnalyzer-2000/2000A RAID settings

Disk #	Size	Status
1	233.76GB	OK
2	233.76GB	Spare
3	233.76GB	OK
4	0.00GB	Not Present
5	233.76GB	OK
6	233.76GB	OK

RAID Level	Select a RAID level from the list. The current RAID level is shown as the first RAID level in the list.
Total Disk Space	The amount of disk space available within the RAID array.
Free Disk Space	The amount of free disk space.
Disk #	The number identifying the disk. These numbers reflect what disks are available on the FortiAnalyzer unit. For example, on a FortiAnalyzer-4000/4000A, there would be 1-12, whereas on a FortiAnalyzer-2000 there would be 1-6.
Size (GB)	The size of the hard disk.
Status	The current status of the hard disk. For example, OK indicates that the hard disk is okay and working normally; Not Present indicates that the hard disk is not being detected by the FortiAnalyzer unit or has been removed and no disk is available; Failed indicates that the hard disk is not working properly.
Apply	Select to apply changes to RAID settings.

Configuring LDAP connections

On the LDAP tab, you can configure an LDAP query to an industry standard LDAP or Windows Active Directory (AD) server.

LDAP queries can be used to create reports whose scope is restricted to include only log messages whose `user=` field matches user names retrieved from an LDAP server. For more information, see [“Configuring reports” on page 113](#).



Caution: By default, the LDAP query occurs over a standard LDAP connection. For secure query (TLS or LDAPS) options, see the [FortiAnalyzer CLI Reference](#).

Figure 34: LDAP settings

The screenshot shows the 'Edit LDAP Server' configuration window. The fields are as follows:

- Name: win_ldap178
- Server Name/IP: 10.10.10.1
- Server Port: 389
- Server Type: Regular
- Bind DN: administrator
- Bind Password: *****
- Common Name Identifier: CN
- Base DN: CN=Users,DC=dev,DC=qa

A checkbox labeled 'LDAP Distinguished Name Query' is checked and highlighted with a blue arrow.

To define an LDAP server query

- 1 Go to **System > Config > LDAP**.
- 2 Select Create New. Complete the following:

Name	Enter the name for the LDAP server query.
Server Name/IP	Enter the LDAP server domain name or IP address.
Server Port	Enter the port number. By default, the port is 389.
Server Type	Select whether to use anonymous or authenticated (regular) queries. If selecting Anonymous, your LDAP server must be configured to allow unauthenticated anonymous queries. If selecting Regular, you must also enter the Bind DN and Bind Password.
Bind DN	Enter an LDAP user name in DN format to authenticate as a specific LDAP user, and bind the query to a DN. This option appears only when the Server Type is Regular.
Bind Password	Enter the LDAP user's password. This option appears only when the Server Type is Regular.
Common Name Identifier	Enter the attribute identifier used in the LDAP query filter. By default, the identifier is <code>cn</code> . For example, if the Base DN contains several objects, and you want to include only objects whose <code>cn=Admins</code> , enter the Common Name Identifier <code>cn</code> and enter the Group(s) value <code>Admins</code> when configuring report profiles. For more information, see "Configuring reports" on page 113 . Report scopes using this query require Common Name Identifier. If this option is blank, the LDAP query for reports will fail.
Base DN	Enter the Distinguished Name of the location in the LDAP directory which will be searched during the query. To improve query speed, enter a more specific DN to constrain your search to the relevant subset of the LDAP tree. For example, instead of entering <code>dc=example,dc=com</code> you might enter the more specific DN <code>ou=Finance,dc=example,dc=com</code> . This restricts the query to the "Finance" organizational unit within the tree. Report scopes using this query require Base DN. If this option is blank, the LDAP query for reports will fail.
LDAP Distinguished Name Query	Select to test the query. Entries in the Base DN appear; if the query results contains multiple levels, entries appear under their parent object.

3 Select OK.

The LDAP query becomes an available option when configuring variables for report profiles. For more information, see [“Configuring reports” on page 113](#).

Maintenance

Maintenance enables you to backup and restore configuration files for the FortiAnalyzer unit, to upload firmware, and to configure automatic RVS updates.

Backup & Restore

Backup & Restore displays the date and time of the last configuration backup and the last firmware upload. It also enables you to:

- download and back up a FortiAnalyzer unit’s configuration
- upload and restore a FortiAnalyzer unit’s configuration
- upload a firmware update

Backup copies of the FortiAnalyzer unit configuration file can be encrypted with a password. When restoring encrypted configuration files, the password must be entered to decrypt the file.



Caution: Do not forget the password to the backup configuration file. A password-encrypted backup configuration file cannot be restored without the password.

For additional information about backing up and restoring configuration, see [“Managing firmware versions” on page 169](#).

Figure 35: Backup & Restore options

The screenshot shows the 'System Configuration' page with the following sections:

- System Configuration (Last Backup: Thu Jun 22 17:31:56 2006)**
- Backup:**
 - Backup configuration to: Local PC (dropdown)
 - Encrypt configuration file
 - Password: [text input]
 - Confirm: [text input]
 - Backup button
- Restore:**
 - Restore configuration from: Local PC (dropdown)
 - Filename: [text input] Browse...
 - Password: [text input]
 - Restore button
- Firmware:**

Partition	Active	Last Upgrade	Firmware Version
1	<input checked="" type="checkbox"/>	Thu Jun 22 12:21:21 2006	FortiAnalyzer-100A 3.00,build341,060621 [Upload and Reboot]

Last Backup

The date and time of the last backup to local PC

Backup

Back up the current configuration.

Backup configuration to: Currently, the only option is to back up to your local PC.

Encrypt configuration file	Select to encrypt the backup file. Enter a password in the Password field and enter it again in the Confirm field. You will need this password to restore the file. You must encrypt the backup file if you are using a secure connection to a FortiGate or FortiManager device.
Backup	Select to back up the configuration.
Restore	Restore the configuration from a file.
Restore configuration from:	Currently the only option is to restore from a PC.
Filename	Enter the configuration file name or use the Browse button if you are restoring the configuration from a file on the management computer.
Password	Enter the password if the backup file is encrypted.
Restore	Select to restore the configuration from the selected file.
Firmware	
Partition	A partition can contain one version of the firmware and the system configuration.
Active	A green check mark indicates which partition contains the firmware and configuration currently in use.
Last Upgrade	The date and time of the last update to this partition.
Firmware Version	The version and build number of the FortiAnalyzer firmware. On the backup partition, you can: <ul style="list-style-type: none"> • Select Upload to replace with firmware from the management computer. • Select Upload and Reboot to replace the firmware.

FortiGuard Center

You can update the engine and vulnerability scan modules in one of the following ways:

- manually upload update packages to the FortiAnalyzer unit from your management computer
- configure the FortiAnalyzer unit to periodically request updates from the Fortinet Distribution Network (FDN)

You must first register the FortiAnalyzer unit with the Fortinet Technical Support web site, <https://support.fortinet.com/> to receive RVS updates from the FDN. The FortiAnalyzer unit must also have a valid Fortinet Technical Support contract, which includes RVS update subscriptions, and be able to connect to the FDN or the IP address that you have configured to override the default FDN addresses. For port numbers required for license validation and update connections, see the Fortinet Knowledge Center article [FDN Services and Ports](#).

For more information about configuring vulnerability scan jobs and viewing vulnerability scan reports, see “Tools” on page 157.

To manually upload RVS updates or to configure scheduled RVS updates, go to **System > Maintenance > FortiGuard Center**.

Figure 36: FortiGuard Center

FortiGuard Subscription Services

The RVS (remote vulnerability scan) engine and module version number, date of last update, and status of the connection to the Fortinet Distribution Network (FDN).

A green indicator means that the FortiAnalyzer unit can connect to the FDN or override server.

A grey indicator means that the FortiAnalyzer unit cannot connect to the FDN or override server. Check the configuration of the FortiAnalyzer unit and any NAT or firewall devices that exist between the FortiAnalyzer unit and the FDN or override server. For example, you may need to add routes to the FortiAnalyzer unit's routing table.

Manual Update

Select to upload an RVS upgrade file from your management computer. To obtain an RVS upgrade file, contact Fortinet Technical Support.

You might upload an RVS file if you want to provide an immediate update, or use an RVS version other than the one currently provided by the FDN. If you want to use an RVS file other than the one currently provided by the FDN, also disable scheduled updates.

Note: Manual updates are not a substitute for a connection to the FDN. Like scheduled updates, manual updates require that the FortiAnalyzer unit be able to connect to the FDN to validate its RVS license.

Remote Vulnerability Scan (RVS)

Select the blue arrow to expand this FortiAnalyzer unit's FortiGuard RVS subscription service options.

Use override server address

Enable Use override server address and enter the IP address and port number of an FDS in the format <IP>:<port>, such as 10.10.1.10:8889.

If you want to connect to a specific FDN server other than the one to which the FortiAnalyzer unit would normally connect, you can override the default IP addresses by configuring an override server.

If, after applying the override server address, the FDN status icon changes to indicate availability (a green check mark), the FortiAnalyzer unit has successfully connected to the override server. If the icon still indicates that the FDN is not available, the FortiAnalyzer unit cannot connect to the override server. Check the FortiAnalyzer configuration and the network configuration to make sure you can connect to the FDN override server from the FortiAnalyzer unit.

Use Web Proxy

Select to enable the FortiAnalyzer unit to connect to the FDN through a web proxy, then enter the IP, Port, and (if required) Name and Password.

IP

Enter the IP address of the web proxy.

Port	Enter the port number of the web proxy. This is usually 8080.
Name	If your web proxy requires a login, enter the user name that your FortiAnalyzer unit should use when connecting to the FDN through the web proxy.
Password	If your web proxy requires a login, enter the password that your FortiAnalyzer unit should use when connecting to the FDN through the web proxy.
Scheduled Update	Enable scheduled updates, then select the frequency of the update (Every, Daily or Weekly).
Every	Select to update once every <i>n</i> hours, then select the number of hours in the interval.
Daily	Select to update once every day, then select the hour. The update attempt occurs at a randomly determined time within the selected hour.
Weekly	Select to update once a week, then select the day of the week and the hour of the day. The update attempt occurs at a randomly determined time within the selected hour.
Request Update Now	Select to immediately request an update.

Device

The Device menu controls connection attempt handling, permissions, disk space quota, and other aspects of devices connecting to the FortiAnalyzer unit for remote logging, content archiving, quarantining, and/or remote management.

For a diagram of traffic types, ports and protocols that FortiAnalyzer units use to communicate with other devices and services, see the Knowledge Center article [Traffic Types and TCP/UDP Ports used by Fortinet Products](#).

This section includes the following topics:

- [Viewing the device list](#)
- [Configuring unregistered device connection attempt handling](#)
- [Manually adding a device](#)
- [Blocking device connection attempts](#)
- [Configuring device groups](#)



Note: Connection attempts *not* handled by the device list include log aggregation, log forwarding, and SNMP traps. For more information about configuring connection handling for those types, see [“Configuring log aggregation” on page 58](#), [“Configuring log forwarding” on page 60](#), and [“Configuring SNMP traps and alerts” on page 136](#).

Viewing the device list

The device list displays devices allowed to connect to the FortiAnalyzer unit and their connection permissions. It may also display unregistered devices attempting to connect.

Connection attempts occur when a device sends traffic to the FortiAnalyzer unit before you have added the device to device list on the FortiAnalyzer unit. FortiAnalyzer units either ignore the connection attempt, or automatically add the device to its device list. This connection attempt handling depends on the type of the device attempting to connect, your selections in Unregistered Device Options, and whether or not the maximum number of devices has been reached on the FortiAnalyzer unit.

- For more information about connection attempt handling, see [“Configuring unregistered device connection attempt handling” on page 79](#).
- For more information about the device number maximum, see [“Maximum number of devices” on page 76](#).
- For more information about manually adding a device to the device list, see [“Manually adding a device” on page 80](#).

You may want to block connection attempts from devices that you do not want to add to the device list since connection attempts must be reconsidered with each attempt. For more information, see [“Blocking device connection attempts” on page 86](#).

Devices may automatically appear on the device list when the FortiAnalyzer receives a connection attempt, according to your configuration of Unregistered Device Options, but devices may also automatically appear as a result of importing log files. For more information, see [“Importing a log file” on page 95](#).

To view the device list, go to **Device > All**.

Figure 1: Devices list

Name	Hardware	IP Address	Log Tx Rx	Content Tx Rx	Quar Tx Rx	Report Tx Rx	Secure Connection	Disk Space (MB) Used/Allocated	Action
FGT-602803030702	FGT-60	172.20.120.149	✓✓	✓✓	✓✓	✓✓	✓	41/1001 MB	[Add] [Edit] [Delete] [Block]
FGT5002801021077	FGT500	172.20.120.132	✓✓	✓✓	✓✓	✓✓	✓	1199/1805 MB	[Add] [Edit] [Delete] [Block]
FGT5002803033050	FGT500	172.20.120.131	✓✓	✓✓	✓✓	✓✓	✓	25/1009 MB	[Add] [Edit] [Delete] [Block]
FWF60A2906501184	FWF60A	0.0.0.0	✓✓	✓✓	✓✓	✓✓	✓	740/1084 MB	[Add] [Edit] [Delete] [Block]
FMG-3K2404400063	FMG-3K	172.20.120.161	✓✓	✓✓	✓✓	✓✓	✓	18/1000 MB	[Add] [Edit] [Delete] [Block]
All_FortiClients	FCT300		✓	⊖	⊖	⊖	⊖	0/1000 MB	[Add] [Edit] [Delete] [Block]
FortiMail-400	FE-400	0.0.0.0	✓	⊖	⊖	⊖	⊖	0/1000 MB	[Add] [Edit] [Delete] [Block]
SYSLOG-172.20.120.46		172.20.120.46	⊗	⊖	⊖	⊖	⊖	0/1000 MB	[Add] [Edit] [Delete] [Block]

Add Device

Select to manually add a new device to the device list.

For instructions on manually adding devices, see [“Manually adding a device” on page 80](#).

Show

Select the type of devices to display in the list. You can select devices by type or by group, or select Unregistered to display devices that are attempting to connect but that have not yet been added.

Page

Enter a page number, then press Enter to display that page number of the device list.

Unregistered Device Options

Select the options to instruct the FortiAnalyzer unit on how to handle connection attempts from unregistered devices. For more information, see [“Configuring unregistered device connection attempt handling” on page 79](#).

Name

The name of the device in the device list. This can be any descriptive name that you want assign to it, and does not need to be its host name.

Hardware

The model of the device. For example, the device list displays a FortiGate-300A model as FGT300A.

IP Address

The IP address of the device. If the device has not recently established a connection, 0.0.0.0 appears.

Administrative Domains

The ADOM(s) to which the device is assigned. This column does not appear on FortiAnalyzer-100/A/B models.

**Log Tx Rx
Content Tx Rx
Quar Tx Rx
Report Tx Rx**

Indicates connection permissions. Green check mark icons in:

- Tx indicates the device is allowed to transmit to the FortiAnalyzer unit.
- Rx indicates the device is allowed to view or retrieve items stored on the FortiAnalyzer unit.

Types of connections supported by each device type vary, and so it is normal for some device types to have no permission in Content (content archive), Quar (quarantine), and Report columns, or to have Tx but not Rx permission in the Log column. For example, Syslog devices are not capable of retrieving logs, and so have no associated Rx permission in the Log column. For FortiManager units, Tx and Rx indicators in the Log column differ in meaning.

- Tx indicates logging access for all devices managed by the FortiManager system.
- Rx indicates that the FortiManager system can remotely administer the FortiAnalyzer unit.

For more information about on configuring device connection permissions, see [“Devices Privileges” on page 82](#).

Secure Connection

Indicates whether an IPSec VPN tunnel has been enabled for secure transmission of logs, content and quarantined files. A locked icon indicates that Secure Connection is enabled.

Enable and configure secure connections in the CLI. The secure tunnel must be configured on both ends of the tunnel: the FortiAnalyzer unit and the device.

Secure Connections cannot be configured with FortiMail units, FortiClient installations, or Syslog devices. For more information on the CLI command, see the [FortiAnalyzer CLI Reference](#).

On a FortiAnalyzer unit:

```
config log device
  edit <devname_str>
    set secure psk
    set psk <presaredkey_str>
    set id <devid_str>
  end
```

On a FortiGate unit:

```
config system fortianalyzer
  set encrypt enable
  set psksecret <presaredkey_str>
  set localid <devname_str>
end
```

On a FortiManager unit:

```
config fmsystem log fortianalyzer
  set secure_connection enable
  set psk <presaredkey_str>
  set localid <devname_str>
end
```

Caution: The locked icon does not indicate successful secure transmission — it only indicates whether the Secure Connection feature is enabled.

For example, if Secure Connection is enabled but not yet configured, the locked icon will appear, but the FortiAnalyzer unit cannot create a secure tunnel without being configured first.

For more information on the secure connection and fallback behavior, see [“Unregistered vs. registered devices” on page 77](#)

Caution: Changing a device’s FortiAnalyzer settings clears sessions to its FortiAnalyzer unit’s IP address. If the FortiAnalyzer unit is behind a NAT device, such as a FortiGate unit, this also resets sessions to other hosts behind that same NAT.

To prevent disruption of other devices’ traffic, on the NAT device, create a separate virtual IP for the FortiAnalyzer unit.

Disk Space (MB) Used/Allocated

The amount of the FortiAnalyzer disk space allocated for the device and how much of that space is used. For more information about on disk space usage by quarantine files, see [“Viewing quarantined files” on page 131](#).

Action

Select Edit to reconfigure the device connection.

Select Delete to remove a device from the list. If the Delete option does not appear for the device, first remove it from all device groups, then delete the device.

For unregistered devices, additional icons appear. Select Add to add the device to the device list and to configure the connection, or select Block to stop further connection attempts. For instructions on manually adding devices, see [“Manually adding a device” on page 80](#). For more information about on blocking a device, see [“Blocking device connection attempts” on page 86](#).

To delete a device

- 1 Go to **Device > All > Device**.
- 2 In the row corresponding to the device that you want to delete, in the Action column, select Delete.

A confirmation dialog appears.

The Delete option may not appear if the device is referenced elsewhere in the configuration, such as by being assigned to a device group. To delete the device, first remove all configuration references to that device.

- 3 Select OK.

The device is removed from the device list and associated log and other data, such as content archives and the default report profile for the device (that is, the device summary report `Default_<device-id>`) are deleted. Reports that may have been already generated from the device's log data, however, are not deleted.

If the device is still configured to attempt to connect to the FortiAnalyzer unit and you have configured Unregistered Device Options to display connection attempts from unregistered devices, the device may reappear in the device list.

Maximum number of devices

Each FortiAnalyzer model is designed to support and provide effective logging and reporting capabilities for up to a certain maximum number of devices (registered and unregistered combined). The following table details these maximums.

Table 7: FortiAnalyzer device limits

	Maximum number of devices and / or VDOMs allowed	Maximum number of FortiClient installations allowed	FortiGate models supported
FortiAnalyzer-100A/100B	100	100	FortiGate-50A to FortiGate-100A
FortiAnalyzer-400/400B	200	2000	FortiGate-50A to FortiGate-800
FortiAnalyzer-800	500	5000	FortiGate-50A to FortiGate-800
FortiAnalyzer-800B	500	5000	FortiGate-50A to FortiGate-3000
FortiAnalyzer-2000/2000A	500	5000	All
FortiAnalyzer-4000	500	10 000	All
FortiAnalyzer-4000A	700	10 000	All

For networks with more demanding logging scenarios, an appropriate device ratio may be less than the allowed maximum. Performance will vary according to your network size, device types, logging thresholds, and many other factors. When choosing a FortiAnalyzer model, consider your network's log frequency, and not only your number of devices.

A VDOM or high availability (HA) cluster counts as a single "device" towards the maximum number of allowed devices. Multiple FortiClient installations (which can number up to the limit of allowed FortiClient installations) also count as a single "device."

For example, a FortiAnalyzer-100B could register up to either:

- 10 devices
- 9 devices and 100 FortiClient installations
- 9 devices and one HA pair
- 1 device and 9 VDOMs

but could *not* register 1 device and 900 FortiClient installations.

When devices attempt to connect to a FortiAnalyzer unit that has reached its maximum number of allowed devices, the FortiAnalyzer unit will reject connection attempts by excess devices, and automatically add those excess devices to the list of blocked devices. For more information about blocked devices, see ["Blocking device connection attempts" on page 86](#).

Once the FortiAnalyzer unit has exceeded its maximum number of allowed devices, you will not be able to add devices to the device list. To resume adding devices, you must first block a device that is currently on your device list, then unblock the device you want to add and add it to the device list.

Unregistered vs. registered devices

The FortiAnalyzer device list can display both registered and unregistered devices.

If you have configured Unregistered Device Options to do so, unregistered devices appear in the device list when the FortiAnalyzer unit receives a connection attempt. However, a device will not be able to use most of the FortiAnalyzer unit's features until you register the device, either manually or automatically.

If you want to configure connection attempt handling, including whether or not a device is automatically added to the device list as a registered or unregistered device, see ["Configuring unregistered device connection attempt handling" on page 79](#).

For more information about manually registering a device, see ["Manually adding a device" on page 80](#).



Note: Both registered and unregistered devices count towards the maximum number of devices available for a FortiAnalyzer unit. Too many unregistered devices will prevent you from adding a device. For more information, see ["Maximum number of devices" on page 76](#).

Configuring unregistered device connection attempt handling

You can configure the FortiAnalyzer unit to accept and handles connection attempts automatically, or to allow connections only from devices that you have manually added.

Allowing the connection and registering the device enables certain FortiAnalyzer features. For example, registering known-type devices, either manually or automatically, configures the FortiAnalyzer unit for features such as device-specific reports and remote browsing of log messages. Manually adding unknown-type devices allows you to browse their logs.

Device connection attempt handling and other FortiAnalyzer features vary by device type. There are two types of devices:

- known device types (FortiGate, FortiManager, FortiClient, FortiMail)
- unknown device type (generic Syslog devices)

Connection attempt handling options for known and unknown device types are separate.

Depending on your settings in Unregistered Device Options, and whether the device type is known or unknown, the FortiAnalyzer unit handles connection attempts in one of these ways:

- ignore the connection (only allow connections from manually added devices)
- allow the connection, add as an *unregistered* device, but do not keep the device's log data (add devices automatically, but do not keep data until you manually register them)
- if the device is an unknown type, allow the connection, add as an *unregistered* device, and keep a specified amount of the device's log data
- if the device is a known type, allow the connection, add as a registered device, and keep a specified amount of the device's log data

If you have specified that connections from unregistered devices will not be allowed until you manually add them, you must manually configure the connection before the device will be allowed to connect to the FortiAnalyzer unit.

When devices attempt to connect to a FortiAnalyzer unit that has reached its number of maximum number of allowed devices, the FortiAnalyzer unit will reject connection attempts by excess devices, and automatically add those excess devices to the list of blocked devices. For more information about on blocked devices, see [“Blocking device connection attempts” on page 86](#).

To view the current connection handling settings, go to **Device > All > Device** and select Unregistered Device Options.



Note: Many FortiAnalyzer features are not available for unregistered devices of unknown types. For more information about on the differences between unregistered and registered devices, see [“Unregistered vs. registered devices” on page 77](#).

Both registered and unregistered devices count towards the maximum number of devices available for a FortiAnalyzer unit. Too many unregistered devices will prevent you from adding a device. For more information, see [“Maximum number of devices” on page 76](#).

Figure 2: Unregistered Device Options

To configure device connection attempt handling

- 1 Go to **Device > All > Device**.
- 2 Select Unregistered Devices Options.
- 3 Select from the following options for *known* device types:

Ignore connection and log data	Do not accept connection attempts, and do not add devices to the device list.
Allow connection, add to unregistered table, but ignore log data	Add the device to the unregistered device list for future configuration and addition to the FortiAnalyzer unit, but do not save the incoming log messages to the hard disk.
Allow connection, register automatically, and store up to <i>N</i> MB data	Add the device to the registered device list for future configuration and addition to the FortiAnalyzer unit, and save the log messages to the hard disk, but only up to <i>N</i> MB disk space.

or the following options for *unknown* device types:

Ignore all unknown unregistered devices	Do not accept any unknown, unregistered incoming device requests, and do not add them to the unregistered device list.
Add unknown unregistered device to unregistered table, but ignore data	Add the device to the unregistered device list for future configuration and addition to the FortiAnalyzer unit, but do not save the incoming log messages to the hard disk.
Add unknown unregistered devices to unregistered table, and store up to <i>N</i> MB data	Add the device to the <i>unregistered</i> device list for future configuration and addition to the FortiAnalyzer unit, and save the log messages to the hard disk, but only up to <i>N</i> MB disk space. Logs cannot be displayed until you add the device to the device list.

- 4 Select OK.

Manually adding a device

You can add devices to the FortiAnalyzer unit's device list either manually or automatically. If you have configured Unregistered Device Options to automatically register known-type devices, you may only need to manually add unknown-type devices such as a generic Syslog server. If you have configured Unregistered Device Options to require it, you may be required to add all devices manually. For more information, see [“Configuring unregistered device connection attempt handling” on page 79](#).

If the device has already been automatically added, the device was added to the device list using default settings. You can reconfigure the device connection by manually editing the device in the device list.

Manually adding a device to the device list, or editing its configuration, configures connections from the device but does not automatically establish a connection. You need to configure the device to send traffic to the FortiAnalyzer unit to establish a connection. For more information, see the [FortiGate Administration Guide](#), [FortiMail Administration Guide](#), [FortiManager Administration Guide](#), [FortiClient Administrator's Guide](#), or your Syslog server's documentation. If there is no explicit option to log specifically to a FortiAnalyzer unit, you can use options for remote logging to a Syslog server.

Due to the nature of connectivity for certain high availability (HA) modes, FortiGate units in an HA cluster may not be able to send full content archives and quarantine data. For more information, see the [FortiGate HA Overview](#).

All FortiClient installations are added as a single device, rather than as one device configuration per FortiClient installation, and their log messages are stored together. Use the FortiAnalyzer reporting features, to obtain network histories for individual FortiClient installations.

You must add the FortiManager system to the FortiAnalyzer device list to remotely administer the FortiAnalyzer unit using a FortiManager system. Additionally, you must also:

- enable web services on the FortiAnalyzer network interface that will be connected to the FortiManager system
- register the FortiAnalyzer unit with the FortiManager system
- be able to connect from your computer to the web-based manager of both the FortiManager system and the FortiAnalyzer unit.

For more information on enabling web services, see [“Administrative Access” on page 45](#). For more information on configuring remote management of FortiAnalyzer units using a FortiManager system, see the [FortiManager Administration Guide](#).



Note: Remote logging from FortiClient installations requires FortiClient 3.0 MR2 or later.

Figure 3: Configuring a device

Device Type	Select the device type. The type is automatically pre-selected if you are adding an unregistered device from the device list, or if you are editing an existing device. Other device options vary by the device type.
Device Name	Enter a name to represent the FortiGate unit, such as FG-1000-1. This can be any descriptive name that you want assign to it, and does not need to be its host name. The device name is automatically pre-entered if you are adding a FortiClient installation.
IP Address	Enter the IP address of the device. This option appears only if Device Type is Syslog.
Device ID	Enter the device ID. Device IDs are usually the serial number of the device, and usually appear on the dashboard of the device's web-based manager. The device ID is automatically pre-entered if you are adding an unregistered device from the device list, or if you are editing an existing device. This option does not appear if Device Type is Syslog or FortiClient.
Mode	Select the high availability (HA) mode of the device. If you are adding a single unit, select Standalone. If you are adding an HA cluster, select HA, then add the device ID of each unit in the cluster to Member IDs. This option appears only if Device Type is FortiGate or FortiManager.
Member IDs	For each member in the HA cluster, enter the device ID of the member and select Add. This option appears only if Mode is HA.
Description	Enter any additional information on the device. Description information appears when you hover the mouse over a device name in the device list.
Allocated Disk Space (MB)	Enter the amount of FortiAnalyzer hard disk space allocated to the device's log and content messages, including quarantined files. For more information about on quarantine file disk quota, see "Viewing quarantined files" on page 131 . The allocated space should be at least 10 times the log rolling size for the Log and Content Archive. For example, if you set the log and content archive log file roll size to 50 MB, allocate at least 500 MB of disk space for the device.

	Amounts following the disk space allocation field indicate the amount of disk space currently being used by the device, and the total amount of disk space currently available on the FortiAnalyzer unit.
When Allocated Disk Space is All Used	Select to either overwrite older files or stop logging to indicate what the FortiAnalyzer unit should do when the allocated disk space has been used.
Devices Privileges	Select the blue arrow to expand the area, then select which types of connections the device is permitted to make. Available permissions vary by device type.
Group Membership	Select the blue arrow to expand the area, then assign the device to a device group or groups. For more information, see “Configuring device groups” on page 88 . This option does not appear if Device Type is FortiClient.
FortiGate Interface Specification	Select the blue arrow to expand the area, then assign each network interface to a network interface class. Traffic between classes determines traffic flow directionality for reports. For more information, see “Classifying FortiGate network interfaces” on page 84 .

To manually add a device or HA cluster

- 1 Go to **Device > All > Device**.
- 2 If the device appears in the device list but is unregistered, from Show, select Unregistered, then in row corresponding to the device, in the Action column, select Add.
Otherwise, select Add Device.
- 3 Select the Device Type.
- 4 If Device Type is not FortiClient, enter the Device Name.
- 5 If Device Type is not Syslog or FortiClient, enter the Device ID.
If the device is a high availability (HA) cluster, enter the device ID of the primary unit.
- 6 If Device Type is Syslog, enter the IP address of the Syslog device.
- 7 If Device Type is FortiGate or FortiManager, from Mode, select either Standalone or HA to indicate the high availability (HA) mode of the device.
If Mode is HA, also add the device ID of each member unit other than the primary unit to Members IDs.
- 8 Enter the Description, if any.
- 9 Enter the device's disk space quota in Allocated Disk Space.
- 10 Select from When Allocated Disk Space is All Used to either Overwrite Oldest Log Files or to Stop Logging.
- 11 Select the blue arrow to expand Devices Privileges.
- 12 Select the connection privileges (Tx and Rx) of the device, such as for sending and viewing log files, content archives and quarantined files. Available device connection privileges vary by Device Type.



Note: Remotely accessing logs, content logs and quarantined files is available on FortiGate units running firmware version 3.0 or later.

- 13 Select the blue arrow to expand Group Membership.
This option does not appear if Device Type is FortiClient. In that case, also skip the following step.
- 14 From the Available Groups area, select a device group or groups, if any, to which you want to assign the device, then select the right arrow button to move the group name into the Membership area.
Devices can belong to multiple groups. You can also add the device to a group later, or change the assigned group. For more information, see [“Configuring device groups” on page 88](#).
- 15 Select the blue arrow to expand FortiGate Interface Specification.
This option appears only if Device Type is FortiGate. If this option does not appear, proceed to the following step.
- 16 Define the functional class of each network interface or VLAN sub-interface.
For more information about how to define the functional class of each network interface or VLAN sub-interface, see [“Classifying FortiGate network interfaces” on page 84](#).
- 17 Select OK.
The device appears in the device list. After registration, some device types can be configured for Secure Connection. For more information, see [“Secure Connection” on page 74](#).

Classifying FortiGate network interfaces

The FortiGate Interface Specification area enables you to functionally classify network interfaces and VLAN subinterfaces according to their connections in your network topology. Functionally classifying the device’s network interfaces and VLAN subinterfaces as None, LAN, WAN or DMZ indirectly defines the directionality of traffic flowing between those network interfaces. For example, FortiAnalyzer units consider log messages of traffic flowing from a WAN class interface to a LAN or DMZ class interface to represent incoming traffic.

Some report types for FortiGate devices include traffic direction — inbound or outbound traffic flow. When the FortiAnalyzer unit generates reports involving traffic direction, the FortiAnalyzer unit compares values located in the source and destination interface fields of the log messages with your defined network interface classifications to determine the traffic directionality.

The table below illustrates the traffic directionality derived from each possible combination of source and destination interface class.

Table 8: Traffic directionality by class of the source and destination interface

Source interface class	Destination interface class	Traffic direction
None	All types	Unclassified
All types	None	Unclassified
WAN	LAN, DMZ	Incoming
WAN	WAN	External
LAN, DMZ	LAN, DMZ	Internal
LAN, DMZ	WAN	Outgoing

To classify network interfaces and VLAN subinterfaces of a FortiGate unit

- 1 Go to **Device > All > Device**.
- 2 Configure the FortiGate device.
For more information, see [“Manually adding a device” on page 80](#).
- 3 Select the blue arrow to expand FortiGate Interface Specifications.
This area may be automatically pre-configured with default classifications. In this case, verify that the network interface classifications match your network topology. If no modification is necessary, select OK, and do not perform the following steps.
- 4 For each network interface, in Available Interfaces, enter the name of the network interface as it appears in log messages, then select Add.
The name of each network interface appears in the Available Interfaces area.
- 5 For each network interface name in the Available Interfaces area, select the name of the network interface, then either leave it in Available Interfaces (which results in a class of None), or move it to the LAN, DMZ, or WAN area using the right arrow for that class.
- 6 From Default type for interfaces not listed here, select None, LAN, WAN, or DMZ to indicate the default class of any network interfaces that you have not manually classified.
- 7 Select OK.

Manually adding a FortiGate unit using the Fortinet Discovery Protocol (FDP)

If you configure the FortiAnalyzer unit to respond to Fortinet Discovery Protocol (FDP) packets, FortiGate units running FortiOS version 3.0 or greater can use FDP to locate a FortiAnalyzer unit. To use FDP, both units must be on the same subnet, and they must be able to connect using UDP.

When a FortiGate administrator selects Automatic Discovery, the FortiGate unit sends FDP packets to locate FortiAnalyzer units on the same subnet. If FDP has been enabled for its interface to that subnet, the FortiAnalyzer unit will respond. Upon receiving an FDP response, the FortiGate unit knows the IP address of the FortiAnalyzer unit, and the administrator can configure the FortiGate unit to begin sending log, content archive, and/or quarantine data to that IP address. When the FortiGate unit attempts to send data to the FortiAnalyzer unit, the FortiAnalyzer unit detects the connection attempt.

Connection attempts from devices not registered with the FortiAnalyzer unit's device list may not be automatically accepted. In this case, you may need to manually add the device to the device list. For more information, see [“Configuring unregistered device connection attempt handling” on page 79](#).

For a diagram of traffic types, ports and protocols that FortiAnalyzer units use to communicate with other devices and services, see the Knowledge Center article [Traffic Types and TCP/UDP Ports used by Fortinet Products](#).



Note: Due to the nature of connectivity for certain high availability (HA) modes, full content archiving and quarantining may not be available for FortiGate units in an HA cluster. For more information, see the [FortiGate HA Overview](#).

Unregistered Device Options apply to all device types attempting to connect, not just FortiGate units.

To enable the FortiAnalyzer unit to reply to FDP packets

- 1 On the FortiAnalyzer unit, go to **Device > All**.
- 2 Go to **System > Network**.
- 3 Select Modify for the network interface that should reply to FDP packets.
- 4 Enable Fortinet Discovery Protocol.
- 5 Select OK.

The FortiAnalyzer unit is now configured to respond to FDP packets on that network interface, including those from FortiGate units' Automatic Discovery feature. For more information about connecting the FortiGate unit using FDP, see ["To connect a FortiGate unit to a FortiAnalyzer unit using FDP" on page 85](#).

To connect a FortiGate unit to a FortiAnalyzer unit using FDP

- 1 On the FortiGate unit, go to **Log&Report > Log Config > Log Setting**.
- 2 Select Remote Logging.
- 3 Select FortiAnalyzer.
- 4 From Minimum log level, select the severity threshold that log messages must meet or exceed to be remotely logged to the FortiAnalyzer unit.
- 5 In the FortiAnalyzer IP area, select Automatic Discovery.
- 6 If the FortiAnalyzer unit does not appear in the Connect To list, select Discover.

The FortiGate unit sends FDP packets to other hosts on the FortiGate unit's subnet. If a FortiAnalyzer unit exists on the subnet and is configured to reply to FDP packets, it sends a reply, and its IP address appears in the Connect To list.

If your FortiGate unit is connecting to a FortiAnalyzer unit from another network, such as through the Internet or through other firewalls, this may fail to locate the FortiAnalyzer unit, and you may need to configure an IPSec VPN tunnel to facilitate the connection. For more information and examples, see the Fortinet Knowledge Center article [Sending remote FortiGate logs to a FortiAnalyzer unit behind a local FortiGate unit](#).

- 7 From the Connect To list, select a FortiAnalyzer unit.
- 8 Select Apply.
- 9 To verify connectivity with the FortiAnalyzer unit, select Test Connectivity.

Test Connectivity verifies connectivity by OFTP. OFTP is required by device registration, content archiving, quarantining, and remote viewing of logs and reports, and display connection permissions, but not to send log messages. If Test Connectivity fails, the FortiAnalyzer unit's Unregistered Device Options may require that you manually register the FortiGate unit with the device list. For more information, see ["Configuring unregistered device connection attempt handling" on page 79](#). For more information about manually registering the device, see ["Manually adding a device" on page 80](#). If the FortiGate unit is registered but Test Connectivity still fails, verify configurations of any intermediate devices such as routers or firewalls.

Test Connectivity does not verify connectivity by Syslog. Syslog is required to send log messages. To verify Syslog connectivity, trigger FortiGate logs, then go to **Log&Report > Log Access > Remote**. Steps required to trigger sending log messages from the FortiGate unit varies by the log type. For example, event logs are not configured in the same location as logs resulting from firewall policies and protection profiles. For more information, see the [FortiGate Administration Guide](#).

When full connectivity is verified, the FortiGate unit can send log and other data to the FortiAnalyzer unit. For more information about configuring FortiGate unit quarantining, content archiving, and/or remote logging, see the [FortiGate Administration Guide](#).

Blocking device connection attempts

Blocking devices prevents them from being able to attempt connections to the FortiAnalyzer unit.

FortiAnalyzer units support a maximum number of devices, including registered and unregistered devices combined. For more information, see [“Maximum number of devices” on page 76](#). You can manually block unregistered devices that you do not want in the FortiAnalyzer device list to free a spot in the device list.





Devices may automatically appear on your list of blocked devices. This can occur when devices attempt to connect after the maximum number of allowed devices has been reached. To resume adding devices, you must first block a device that is currently on your device list, then unblock the device you want to add, and add it to the device list.

To view blocked devices, go to **Device > All > Blocked Devices**.



Note: See [“Configuring unregistered device connection attempt handling” on page 79](#) to prevent unregistered devices from automatically appearing in the device list.

Figure 4: List of blocked devices

Device ID	Hardware Model	IP Address	Action
SYSLOG-172.20.120.46	Syslog	172.20.120.46	 
FGT-602803030702	FortiGate	172.20.120.149	 

Delete
Unblock

Device ID	The name or serial number of the blocked device.
Hardware Model	The type of device, such as FortiGate, FortiManager, FortiMail, or Syslog server.
IP Address	The IP address of the blocked device.
Action	Select Delete to remove the device from the list of blocked devices. If the device attempts to connect to the FortiAnalyzer unit, it may appear in the device list as an Unregistered device, according to your configuration of Unregistered Device Options. For more information, see “Configuring unregistered device connection attempt handling” on page 79 . Select Unblock to add the device to the FortiAnalyzer unit’s device list. For more information, see “Viewing the device list” on page 73 .

To block a device

- 1 Go to **Device > All > Device**.

- 2 From Show, select Unregistered.

If the device is currently registered, you must first delete the device before you can block it. For more information, see [“Viewing the device list” on page 73](#).

- 3 In the row corresponding to the device that you want to block, in the Action column, select Block.

The device appears in the list of blocked devices.

To unblock a device

- 1 Go to **Device > All > Blocked Device**.

- 2 In the row corresponding to the device that you want to remove from the list of blocked devices, select Delete.

A confirmation dialog appears.

- 3 Select OK.

The device is removed from the list of blocked devices. If the device attempts to connect to the FortiAnalyzer unit, it may appear in the device list as an Unregistered device, according to your configuration of Unregistered Device Options. For more information, see [“Configuring unregistered device connection attempt handling” on page 79](#).

To unblock and add a device to the device list

- 1 Go to **Device > All > Blocked Device**.

- 2 In the row corresponding to the device that you want to remove from the list of blocked devices, select Unblock.

A dialog appears, allowing you to add the device to the device list. If the device is a known type, this also registers the device. To add the device to the device list, see [“To manually add a device or HA cluster” on page 82](#).


Configuring device groups

When you have multiple devices belonging to a department or section of your organization, you may want to create device groups to simplify log browsing or report configuration.

A device can belong to multiple groups. However, the device cannot be deleted from the device list until it is removed from all groups.

To view device groups, go to **Device > Group > Device Group**.

Figure 5: List of device groups

Group Name	Members	Modify
tdevgroup	FG200A2907500558, FG36002804033100	 

Delete
Edit

Create New	Select to configure a new device group.
Show	Select the type of device groups to display, such as FortiGate, FortiManager, FortiMail or Syslog groups.
Group Name	The name of the device group.
Members	The device names of devices that are members of the device group.
Modify	Select Delete to remove the device group. Select Edit to reconfigure the device group.

To configure a device group

- 1 Go to **Device > Group > Device Group**.
- 2 Select Create New to configure a new device group, or select Edit to reconfigure an existing device group.
- 3 In Group Name, enter a name for the group.
- 4 From Group Type, select the type of devices in the group.
FortiClient installations are treated as a single device, and so cannot be configured as a device group.
- 5 Select the devices to include in the group from the list of Available Devices and select the right-pointing arrow.
- 6 Select OK.

To delete a device group

- 1 Go to **Device > Group > Device Group**.
- 2 In the row corresponding to the device group that you want to delete, in the Modify column, select Delete.
A confirmation dialog appears.
- 3 Select OK.

Log

FortiAnalyzer units collect logs from network hosts such as FortiGate, FortiMail, FortiClient, FortiManager, and Syslog devices. By using the Log menu, you can view both device and FortiAnalyzer log files and messages, as well as content archive summaries. The FortiAnalyzer unit can display device logs in real-time, enabling you to view log messages as the FortiAnalyzer unit receives them.

This section includes the following topics:

- [Viewing log messages](#)
- [Browsing log files](#)
- [Customizing the log view](#)
- [Searching the logs](#)
- [Rolling and uploading logs](#)



Note: FortiAnalyzer units cannot display logs from unregistered devices of unknown types. Add the device first to view the logs of an unknown type device. For more information about adding a device to the device list, see [“Manually adding a device” on page 80](#).

Viewing log messages

The Log Viewer displays logs for devices that were added to the device list, as well as the FortiAnalyzer unit itself, focusing on specific log types and time frames.

The Log Viewer has two types of log viewing options:

- The Real-time tab displays the log messages most recently received by the FortiAnalyzer unit. The display refreshes every few seconds, and contains only the most current entries.
- The Historical tab displays all log messages for the selected log type whose time stamps are within your specified time frame.

Viewing current log messages

The Real-time tab in **Log > Log Viewer** updates continually, displaying the most recent log messages received from the selected device.

To view the most recent logs as they are received from **Log > Log Viewer > Real-time**.

For more information about log messages, see the [FortiGate Log Message Reference](#).

Figure 1: Viewing current logs

Column Settings

Log Time	Level	Action	Status	Message
2008-07-16 07:00:55	alert	login	failure	User admin login failed from GUI(172.20.120.25)
2008-07-16 07:00:55	alert	login	failed	User admin login failed due to invalid password
2008-07-08 14:06:53	notice	connect	success	Connected to FortiAnalyzer 172.20.120.139
2008-07-08 14:06:51	notice	add-vdom		Virtual domain root is added
2008-07-08 14:06:09	critical	reboot		User admin rebooted the device from GUI(172.20.120.25). The reason is 'for FGAMS connectivity'
2008-07-08 13:34:50	alert	login	failed	Administrator admin login failed from https(172.20.120.25) because of invalid password
2008-07-08 13:25:14	notice	connect	success	Connected to FortiAnalyzer 172.20.120.139
2008-07-08 12:21:35	notice	connect	success	Connected to FortiAnalyzer 172.20.120.139
2008-07-08 09:07:22	notice	connect	success	Connected to FortiAnalyzer 172.20.120.139
2008-07-08 09:07:20	notice	add-vdom		Virtual domain root is added
2008-07-08 09:05:23	critical	reboot		User admin rebooted the device from GUI(172.20.120.25). The reason is 'upgrade firmware'
2008-07-08 09:05:23	critical	restore-image	success	User admin restored the image from GUI(172.20.120.25) (3.00.0660 -> 3.0.716)
2008-07-08 09:05:23	critical	loaded-image	success	User admin loaded an image from GUI(172.20.120.25). The new image does have a valid RSA signature.
2008-07-08 09:04:40	critical			FortiGuard - AV Query license is expired
2008-07-08 09:04:40	critical			FortiGuard - AntiSpam license is expired
2008-07-08 09:04:40	critical			FortiGuard Web Filter license is expired.
2008-07-08 09:04:40	notice	connect	success	Connected to FortiAnalyzer 172.20.120.139
2008-07-08 09:04:29	notice	add-vdom		Virtual domain root is added
2008-07-08 08:02:39	warning	download	success	System config file has been downloaded by user admin via GUI(172.20.120.25)
2008-07-08 08:00:36	warning	download	success	System config file has been downloaded by user admin via GUI(172.20.120.25)
2008-07-07 12:13:44	alert	login	failure	User admin login failed from GUI(172.20.120.25)
2008-07-07 12:13:44	alert	login	failed	User admin login failed due to invalid password
2008-06-16 09:50:05	notice	connect	success	Connected to FortiAnalyzer 172.20.120.139
2008-06-16 09:50:05	notice	disconnect	success	Disconnected from FortiAnalyzer 172.20.120.139
2008-06-16 08:34:30	information	perf-stats		Performance statistics
2008-06-16 08:32:32	information	logout	success	Administrator admin logged out from https(172.20.120.25)
2008-06-16 08:29:30	information	perf-stats		Performance statistics
2008-06-16 08:24:30	information	perf-stats		Performance statistics
2008-06-16 08:19:30	information	perf-stats		Performance statistics
2008-06-16 08:16:52	information	login	success	Administrator admin logged in successfully from ssh(172.20.120.25)

- Devices** Select the type of device you want to view logs from. If you select All FortiGates, all log messages from all registered FortiGate units appear.
- Log types** Select to view a different device's logs, or a different log type.
- Stop** Select to stop refreshing the log view. This option appears only when refreshing is started.
- Start** Select to start refreshing the log view. This option appears only when refreshing is stopped.
- Column Settings** Select to change the columns to view and the order they appear on the page. For more information, see ["Displaying and arranging log columns" on page 97](#).
- Formatted | Raw** Select a view of the log file. Selecting Formatted (the default) displays the log files in columnar format. Selecting Raw, displays the log information as it actually appears in the log file.
- View *n* per page** Select the number of rows of log entries to display per page. You can choose up to 1000 entries.



Note: Log messages that are received from a log aggregation device are scheduled transfers, and not real-time messages, because log aggregation devices do not appear in the Real-time tab. Individual high availability (HA) cluster members also do not appear in the Real-time tab because HA members are treated as a single device.

Viewing historical log messages

The Historical tab in **Log > Log Viewer** displays logs for a selected device and log type for a specific time range. When viewing log messages, you can filter the information to find specific event information.

For more information about log messages, see the [FortiGate Log Message Reference](#).

Figure 2: Viewing historical logs

Column Settings Printable Version

#	Last Activity	Level	Action	Status	Message
1	2007-02-16 05:32:04	information	logout	success	User admin terminates the session from jsonconsole
2	2007-02-16 05:32:04	information	logout	success	User admin terminates the session from jsonconsole
3	2007-02-16 02:32:04	information			Client requests IP address/configuration parameters
4	2007-02-16 02:32:04	error	negotiate	negotiate_error	Parse ISAKMP error: unsupported OAKLEY attribute
5	2007-02-16 02:32:04	information			Client requests IP address/configuration parameters
6	2007-02-16 02:32:04	error	negotiate	negotiate_error	Parse ISAKMP error: unsupported OAKLEY attribute
7	2007-02-15 23:32:04	warning	content-archive	drop	File '00370a06.a.617' is not transferred to FortiAnalyzer due to exceeding memory usage limit.
8	2007-02-15 23:32:04	warning	content-archive	drop	File '00370a06.a.617' is not transferred to FortiAnalyzer due to exceeding memory usage limit.
9	2007-02-15 20:32:04	error	dpd	dpd_failure	IPsec DPD detected a failure on the tunnel to 203.211.130.500
10	2007-02-15 20:32:04	critical			FortiGuard - AntiSpam license is expired
11	2007-02-15 20:32:04	error	dpd	dpd_failure	IPsec DPD detected a failure on the tunnel to 203.211.130.500
12	2007-02-15 20:32:04	critical			FortiGuard - AntiSpam license is expired
13	2007-02-15 17:32:04	alert	login	failure	User admin login failed from GUI(172.16.1.20)
14	2007-02-15 17:32:04	notice		update	Fortigate push update virdb(6.817) idsdb(2.331) aven(2.002) idsen(1.035) from: 203.211.130.500:443
15	2007-02-15 17:32:04	alert	login	failure	User admin login failed from GUI(172.16.1.20)
16	2007-02-15 17:32:04	notice		update	Fortigate push update virdb(6.817) idsdb(2.331) aven(2.002) idsen(1.035) from: 203.211.130.500:443
17	2007-02-15 04:26:18	error	dpd	dpd_failure	IPsec DPD detected a failure on the tunnel to 203.211.130.500
18	2007-02-15 04:26:18	error	dpd	dpd_failure	IPsec DPD detected a failure on the tunnel to 203.211.130.500
19	2007-02-15 01:26:18	information			Client requests IP address/configuration parameters
20	2007-02-15 01:26:18	information			Assigns IP address/configuration parameters to the client
21	2007-02-15 01:26:18	information			Client requests IP address/configuration parameters
22	2007-02-15 01:26:18	information			Assigns IP address/configuration parameters to the client
23	2007-02-14 22:26:18	emergency			Disk logs exceed 95% of disk size.Deleted rolled log file name tlog.76.
24	2007-02-14 22:26:18	emergency			Disk logs exceed 95% of disk size.Deleted rolled log file name tlog.76.
25	2007-02-14 19:26:18	notice	negotiate	success	Initiator: tunnel 219.133.5.246, transform=ESP_3DES, HMAC_SHA1
26	2007-02-14 19:26:18	notice	negotiate	success	Initiator: tunnel 219.133.5.246, transform=ESP_3DES, HMAC_SHA1
27	2007-02-14 16:26:18	notice	delete_ipsec_sa		Deleted an IPsec SA on the tunnel to 203.211.130.500
28	2007-02-14 16:26:18	notice	delete_ipsec_sa		Deleted an IPsec SA on the tunnel to 203.211.130.500
29	2007-02-14 03:10:19	notice	negotiate	success	Initiator: sent 203.211.130.500 quick mode message #1 (OK)
30	2007-02-14 03:10:19	notice	negotiate	success	Initiator: sent 203.211.130.500 quick mode message #1 (OK)

Devices	Select the type of device you want to view logs from. If you select All FortiGates, all log messages from all registered FortiGate units appear.
Log Types	Select to view a different device's logs, or a different log type.
Formatted Raw	Select a view of the log file. Selecting Formatted (the default) displays the log files in columnar format. Selecting Raw, displays the log information as it actually appears in the log file.
View <i>n</i> per page	Select the number of rows of log entries to display per page. You can choose up to 1000 entries.
Page <i>n</i> of <i>n</i>	Enter a log page number, then press Enter to go to that page.
Column Settings	Select to change the columns to view and the order they appear on the page. For more information, see "Displaying and arranging log columns" on page 97.
Search	Enter a keyword to perform a simple search on the log information available. Select Go to begin the search. The number of matches appears above the Search field. The FortiAnalyzer unit will search the entire log data for the keyword you enter.
Printable Version	Select to download an HTML file containing all log messages that match the current filters. The HTML file is formatted to be printable. Time required to generate and download large reports varies by the total amount of log messages, the complexity of any search criteria, the specificity of your column filters, and the speed of your network connection.
Download Current View	Select to download only those log messages which are currently visible, according to enabled filters. This button appears only when the current view is filtered. The downloaded version will match the current log view, containing only log messages that match your current filter settings.

To view historical logs

- 1 Go to **Log > Log Viewer > Historical**.
- 2 From Devices, select the device whose logs you want to view.
Unregistered devices will not appear in the list. To view a device's logs, you must register the device first.
- 3 From Log types, select the type of log file.
Log types options vary by device type. If you have reason to expect log messages to appear for the selected log type, but none appear, verify connectivity and the device's logging configuration.
- 4 Select OK.

Browsing log files

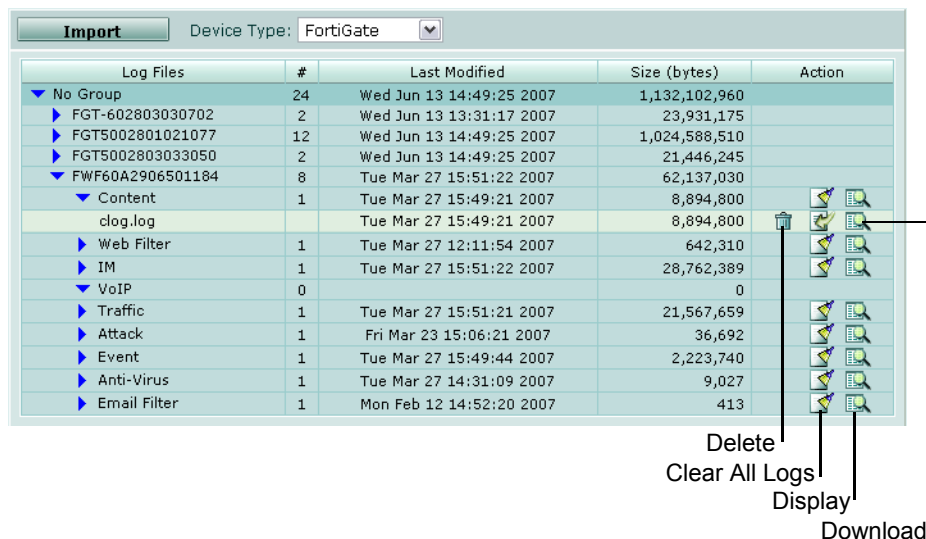
The Log Browser tab enables you to see all stored log files for all devices and the FortiAnalyzer itself. In this window, you can view the log information, download log files to your hard disk, or delete unneeded files.

When a log file reaches its maximum size, the FortiAnalyzer unit saves the log files with an incremental number and starts a new log file with the same name. The current attack log is `alog.log`. Any subsequent saved logs appear as `alog.n.log`, where *n* is the number of rolled logs.

For information about setting the maximum file size and log rolling options, see ["Rolling and uploading logs" on page 104](#).

To browse the log files, go to **Log > Browse**.

Figure 3: Log file list



- Import** Select to import older log files to view and run log reports. For more information about on importing log files, see ["Importing a log file" on page 95](#).
- Device Type** Select a device category to view its related log files.

Log files	A list of available log files for each device or device group. Select the group name to expand the list of devices within the group, and to view their log files. The current, or active, log file appears as well as rolled log files. Rolled log files include a number in the file name (alog.2.log). If you configure the FortiAnalyzer unit to upload rolled logs to an FTP site, only the current log will appear in the log browser.
#	The number of devices in a group, and the number of logs for a device.
Last Modified	The last time the log was updated from the device.
Size (bytes)	The size of the log file.
Action	Select Delete to remove the log file from the FortiAnalyzer hard disk. Select Clear All Logs to delete all log messages within the log file. Select Download to save the log file to your local hard disk. Select Display to view the contents of the log file.

Viewing log file contents

The Log Browser tab enables you to view all log messages within local or device log files.

If you display the log messages in Formatted view, you can display and arrange columns and/or filter log messages by column contents. For more information, see [“Customizing the log view” on page 97](#).

For more information about log messages, see the [FortiGate Log Message Reference](#).



Note: For content archive logs, the log browser only displays the device's clog.log file. It does not provide access to download the archived files. To both view content archive logs and download the associated content archived files, instead go to **Content Archive**. For more information, see [“Content Archive” on page 107](#).

To view a log file

- 1 Go to **Log > Browse**.
- 2 Select the blue arrows to expand the group name and device name to see the list of available log files.
- 3 In the Action column, select Display for that log file's row.

The log file's contents appear.

Figure 4: Viewing logs

Column Settings Printable Version

#	Last Activity	Level	User Interface	Action	Message	Subtype
1	2007-04-26 12:59:46	notice		delete_ipsec_sa	Deleted an IPsec SA on the tunnel to 172.20.120.139:500	ipsec
2	2007-04-26 12:59:18	notice		negotiate	Initiator: sent 172.20.120.139 quick mode message #1 (OK)	ipsec
3	2007-04-26 12:55:59	warning	GUI(172.20.120.46)	download	System config file has been downloaded by user admin via GUI(172.20.120.46)	admin
4	2007-04-26 12:53:11	notice	GUI(172.20.120.46)		User admin added local user user2 from GUI(172.20.120.46)	admin
5	2007-04-26 12:53:01	notice	GUI(172.20.120.46)		User admin added local user user from GUI(172.20.120.46)	admin
6	2007-04-26 12:36:55	information	GUI(172.20.120.46)	login	Administrator admin logged in successfully from GUI(172.20.120.46)	admin
7	2007-04-26 12:30:09	notice		delete_ipsec_sa	Deleted an IPsec SA on the tunnel to 172.20.120.139:500	ipsec
8	2007-04-26 12:29:46	notice		negotiate	Initiator: sent 172.20.120.139 quick mode message #1 (OK)	ipsec
9	2007-04-26 12:00:33	notice		delete_ipsec_sa	Deleted an IPsec SA on the tunnel to 172.20.120.139:500	ipsec
10	2007-04-26 12:00:09	notice		negotiate	Initiator: sent 172.20.120.139 quick mode message #1 (OK)	ipsec
11	2007-04-26 10:30:59	notice		delete_ipsec_sa	Deleted an IPsec SA on the tunnel to 172.20.120.139:500	ipsec
12	2007-04-26 10:30:33	notice		negotiate	Initiator: sent 172.20.120.139 quick mode message #1 (OK)	ipsec
13	2007-04-26 09:31:26	notice		delete_ipsec_sa	Deleted an IPsec SA on the tunnel to 172.20.120.139:500	ipsec
14	2007-04-26 09:30:59	notice		negotiate	Initiator: sent 172.20.120.139 quick mode message #1 (OK)	ipsec
15	2007-04-26 08:44:14	information	GUI(172.20.120.156)	login	Administrator admin logged in successfully from GUI(172.20.120.156)	admin
16	2007-04-26 08:35:45	notice		delete_phase1_sa	Deleted an Isakmp SA on the tunnel to 172.20.120.139:500	ipsec

Type	The type of log you are viewing and the device where it originated.
Change	Select to view a different log file.

Formatted Raw	Select a view of the log file. Selecting Formatted (the default) displays the log files in columnar format. Selecting Raw, displays the log information as it actually appears in the log file.
Resolve Host Name	Select to display host names by a recognizable name rather than IP addresses. For more information about on configuring IP address host names see “Configuring IP aliases” on page 61 .
Resolve Service	Select to display the network service names rather than the port numbers, such as HTTP rather than port 80. This option does not appear when the logs do not have service information to display, which can occur in the event log.
View <i>n</i> per page	Select the number of rows of log entries to display per page.
Page <i>n</i> of <i>n</i>	Enter a log page number, then press Enter to go to that page.
Column Settings	Select to change the columns to view and the order they appear on the page. For more information, see “Displaying and arranging log columns” on page 97 .
Search	Enter a keyword to perform a simple search for that term, then select Go to begin the search. The FortiAnalyzer unit searches the entire log file for the keyword you enter. The number of matches appears above the Search field.
Printable Version	Select to download an HTML file containing all log messages that match the current filters. The HTML file is formatted to be printable. Time required to generate and download large reports varies by the total amount of log messages, the complexity of any search criteria, the specificity of your column filters, and the speed of your network connection.
Download Current View	Select to download only those log messages which are currently visible, according to enabled filters. This button only appears when the current log view is filtered. The downloaded version will match the current log view, containing only log messages that match your current filter settings.

Importing a log file

You can import devices' log files. This 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 onto the FortiAnalyzer unit in order to generate reports on older data. Importing log files is also useful when changing your RAID configuration. Changing your RAID configuration reformats the hard disk, erasing log files. If you back up the log files, after changing the RAID configuration, you can import logs to restore them to the FortiAnalyzer unit.

You can import logs in normal log, compressed log (.log.gz) or comma separated value (CSV) format.

To import a log file

- 1 Go to **Log > Browse**.
- 2 Select the Device Type.
- 3 Select Import.
- 4 Select from Device to which device in the device list the imported log file belongs, or select Take From Imported File to read the device ID from the log file.

If you select Take From Imported File, your log file must contain a `device_id` field in its log messages.

5 In Filename, enter the path and file name of the log file, or select Browse.

6 Select OK.

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

7 Select OK.

Upload time varies by the size of the file and the speed of the connection.

After the log file successfully uploads, the FortiAnalyzer unit inspects the log file.

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

Downloading a log file

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

To download a whole log file

- 1 Go to **Log > Browse**.
- 2 In the Log Files column, locate a device and log type and then select blue arrows to expand and reveal the specific log file (`wlog.log`, `elog.log`, etc.) that you want to download.
- 3 In the Action column, select Download for that log file's row.
- 4 Select any download options you want and select OK.

Convert to CSV format

Downloads the log format as a comma-separated value (`.csv`) file instead of a standard `.log` file. Each log element is separated by a comma. CSV files can be viewed in spreadsheet applications.

Compress with gzip

Compress the `.log` or `.csv` file with gzip compression. For example, downloading a log-formatted file with gzip compression would result in a download with the file extension `.log.gz`.

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

To download a partial log file

- 1 Go to **Log > Browse**.
- 2 In the Log Files column, locate a device and log type and then select blue arrows to expand and reveal the specific log file (`wlog.log`, `elog.log`, etc.) that you want to download.
- 3 In the Action column, select Display for that log file's row.
- 4 Select a filter icon to restrict the current view to only items which match your criteria, then select OK.

Filtered columns have a green filter icon, and Download Current View appears next to Printable Version. For more information about filtering log views, see ["Filtering logs" on page 98](#).

- 5 Select Download Current View.
- 6 Configure the following:

Convert to CSV format	Downloads the log format as a comma-separated value (.csv) file instead of a standard .log file. Each log element is separated by a comma. CSV files can be viewed in spreadsheet applications.
Compress with gzip	Compress the .log or .csv file with gzip compression. For example, downloading a log-formatted file with gzip compression would result in a download with the file extension .log.gz.
- 7 Select OK.
- 8 If prompted by your web browser, select a location to save the file, or open it without saving.

Customizing the log view

Log messages can be displayed in either Raw or Formatted view.

- Raw view displays log messages exactly as they appear in the log file.
- Formatted view displays log messages in a columnar format. Each log field in a log message appears in its own column, aligned with the same field in other log messages, for rapid visual comparison. When displaying log messages in Formatted view, you can customize the log view by hiding, displaying and arranging columns and/or by filtering columns, refining your view to include only those log messages and fields that you want to see.

To display logs in Raw or Formatted view

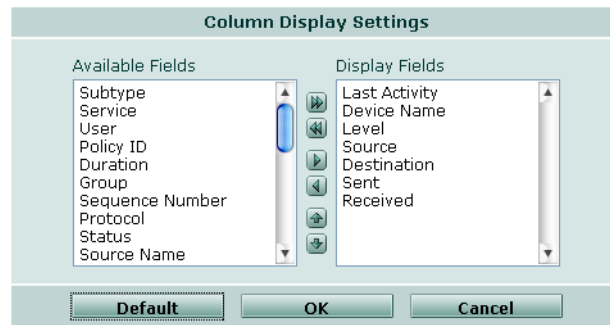
- 1 Go to a page which displays log messages, such as **Log > Log Viewer > Real-time**.
- 2 Select Formatted or Raw.

If you select Formatted, options appear that enable you to display and arrange log columns and/or filter log columns.

Displaying and arranging log columns

When viewing logs in Formatted view, you can display, hide and re-order columns to display only relevant categories of information in your preferred order.

For most columns, you can also filter data within the columns to include or exclude log messages which contain your specified text in that column. For more information, see [“Filtering logs” on page 98](#).

Figure 5: Displaying and arranging log columns**To display or hide columns**

- 1 Go to a page which displays log messages, such as **Log > Log Viewer > Real-time**.
- 2 Select Column Settings.
Lists of available and displayed columns for the log type appear.
- 3 Select which columns to hide or display.
 - In the Available Fields area, select the names of individual columns you want to display, then select the single right arrow to move them to the Display Fields area.
Alternatively, to display all columns, select the double right arrow.
 - In the Display Fields area, select the names of individual columns you want to hide, then select the single left arrow to move them to the Available Fields area.
Alternatively, to hide all columns, select the double left arrow.
 - To return all columns to their default displayed/hidden status, select Default.
- 4 Select OK.

To change the order of the columns

- 1 Go to a page which displays log messages, such as **Log > Log Viewer > Real-time**.
- 2 Select Column Settings.
Lists of available and displayed columns for the log type appear.
- 3 In the Display Fields area, select a column name whose order of appearance you want to change.
- 4 Select the up or down arrow to move the column in the ordered list.
Placing a column name towards the top of the Display Fields list will move the column to the left side of the Formatted log view.
- 5 Select OK.

Filtering logs

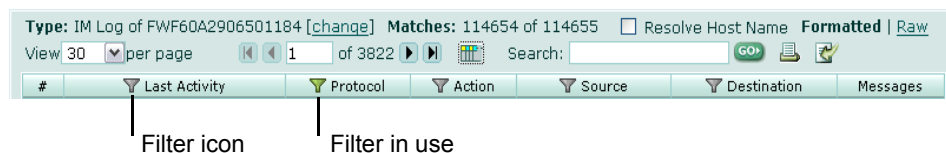
When viewing log messages in Formatted view, you can filter columns to display only those log messages that do or do not contain your specified content in that column. By default, most column headings contain a gray filter icon, which becomes green when a filter is configured and enabled.



Note: Filters do not appear in Raw view, or for unindexed log fields in Formatted view.

When viewing real-time logs, you cannot filter on the time column: by definition of the real-time aspect, only current logs are displayed.

Figure 6: Filter icons



To filter log messages by column contents

- 1 In the heading of the column that you want to filter, select the filter icon.
- 2 Select Enable.
- 3 If you want to *exclude* log messages with matching content in this column, select NOT.

If you want to *include* log messages with matching content in this column, deselect NOT.

- 4 Enter the text that matching log messages must contain.

Matching log messages will be excluded or included in your view based upon whether you have selected or deselected NOT.

- 5 Select OK.

A column's filter icon is green when the filter is currently enabled. A Download Current View icon also appears, enabling you to download only log messages which meet the current filter criteria.

To disable a filter

- 1 In the heading of the column whose filter you want to disable, select the filter icon. A column's filter icon is green when the filter is currently enabled.
- 2 To disable the filter on this column, deselect Enable. Alternatively, to disable the filters on all columns, select Clear All Filters. This disables the filter; it does not delete any filter text you might have configured.
- 3 Select OK.

A column's filter icon is gray when the filter is currently disabled.

Filtering tips

When filtering by source or destination IP, you can use the following in the filtering criteria:

- a single address (2.2.2.2)
- an address range using a wild card (1.2.2.*)
- an address range (1.2.2.1-1.2.2.100)

You can also use a Boolean operator (or) to indicate mutually exclusive choices:

- 1.1.1.1 or 2.2.2.2
- 1.1.1.1 or 2.2.2.*

- 1.1.1.1 or 2.2.2.1-2.2.2.10

Most column filters require that you enter the column's entire contents to successfully match and filter contents; partial entries do not match the entire contents, and so will not create the intended column filter.

For example, if the column contains a source or destination IP address (such as 192.168.2.5), to create a column filter, enter the entire IP address to be matched. If you enter only one octet of the IP address, (such as 192) the filter will not completely match any of the full IP addresses, and so the resulting filter would omit all logs, rather than including those logs whose IP address contains that octet.

Exceptions to this rule include columns that contain multiple words or long strings of text, such as messages or URLs. In those cases, you may be able to filter the column using a substring of the text contained by the column, rather than the entire text contained by the column.

Searching the logs

You can search the device log files for matching text using two search types: Quick Search and Full Search.

You can use Quick Search to find results more quickly if your search terms are relatively simple and you only need to search indexed log fields. Indexed log fields are those that appear with a filter icon when browsing the logs in column view; unindexed log fields do not contain a filter icon for the column or do not appear in column view, but do appear in the raw log view. Quick Search keywords cannot contain:

- special characters such as single or double quotes (` ` or ` `) or question marks (?)
- wild card characters (*), or only contain a wild card as the last character of a keyword (logi*)

You can use Full Search if your search terms are more complex, and require the use of special characters or log fields not supported by Quick Search. Full Search performs an exhaustive search of all log fields, both indexed and unindexed, but is often slower than Quick Search.

Figure 7: Log Search

Device/Group	Select to search logs from the FortiAnalyzer unit (LocalLogs), a device, or a device group.
Date	Select to search logs from a time frame, or select Specify and define a custom time frame by selecting the From and To date and times.
From	Enter the date and select the time of the beginning of the custom time range. This option appears only when Date is Specify.
To	Enter the date and select the time of the end of the custom time range. This option appears only when Date is Specify
Keyword(s)	Enter search terms which will match to yield log message search results. To specify that results must include all, any, or none of the keywords, select these options in Match.
Quick Search	Select to perform a Quick Search. Keywords for a Quick Search cannot contain special characters. Quick Search examines only indexed fields.
Full Search	Select to perform a Full Search. Keywords for a Full Search may contain special characters. Full Search examines all log message fields.
More Options	Select the blue arrow to hide or expand additional search options.
Match	Select how keywords are used to match log messages which comprise search results. <ul style="list-style-type: none"> • All Words: Select to require that matching log messages must contain all search keywords. If a log message does not contain one or more keywords, it will not be included in the search results. • Any Words: Select to require that matching log messages must contain at least one of the search keywords. Any log message containing one or more keyword matches will be included in the search results. • Does Not Contain the Words: Select to require that matching log messages must not contain the search keywords. If a log message contains any of the search keywords, it will be excluded from the search results.
Other Filters	Specify additional criteria, if any, that can be used to further restrict the search criteria. <ul style="list-style-type: none"> • Log Type: Select to include only log messages of the specified type. For example, selecting Traffic would cause search results to include only log messages containing <code>type=traffic</code>. • Log Severity: Select to include only log messages of the specified severity. For example, selecting Notice would cause search results to include only log messages containing <code>pri=notice</code>. • Source IP: Enter an IP address to include only log messages containing a matching source IP address. For example, entering <code>192.168.2.1</code> would cause search results to include only log messages containing <code>src=192.168.2.1</code> and/or content log messages containing a client IP address of <code>192.168.2.1</code>.

- **Destination IP:** Enter an IP address to include only log messages containing a matching destination IP address. For example, entering `192.168.2.1` would cause search results to include only log messages containing `dst=192.168.2.1` and/or content log messages containing a server IP address of `192.168.2.1`.
- **User Name:** Enter a user name to include only log messages containing a matching authenticated firewall user name. For example, entering `userA` would cause search results to include only log messages containing `user="userA"`.
- **Group Name:** Enter a group name to include only log messages containing a matching authenticated firewall group name. For example, entering `groupA` would cause search results to include only log messages containing `group="groupA"`.

To search the logs

- 1 Go to **Log > Search**.
- 2 From Device/Group, select which device or device group's logs you want to search.
- 3 From Date, select Any time to search log messages from all time periods, select a predefined time period, or select Specify and then define the starting and ending time of your custom time period.
- 4 In Keyword(s), enter your search criteria.
- 5 If you want to specify additional match or filter criteria, select More Options to expand that area, then configure those options.
- 6 Select Quick Search or Full Search.

Time required to retrieve search results varies by the complexity of the search query, the amount of log data being searched, and whether you select Quick Search or Full Search.

When the search results display, you can view the log messages in either Format or Raw formats.

Search tips

If your search does not return the results you expect, but log messages exist that should contain matching text, examine your keywords and filter criteria using the following search characteristics and recommendations.

- Separate multiple keywords with a space (`type=webfilter subtype=activexfilter`).
- Keywords cannot contain unsupported special characters. Supported characters vary by selection of Quick Search or Full Search.
- Keywords must literally match log message text, with the exception of case insensitivity and wild cards; resolved names and IP aliases will not match.

- Some keywords will not match unless you include both the log field name and its value (`type=webfilter`).
- Remove unnecessary keywords and search filters which can exclude results. In More Options, if All Words is selected, for a log message to be included in the search results, *all* keywords must match; if any of your keywords do not exist in the message, the match will fail and the message will not appear in search results. If you cannot remove some keywords, select Any Words.
- You can use the asterisk (*) character as a wild card (`192.168.2.*`). For example, you could enter any partial term or IP address, then enter * to match all terms that have identical beginning characters or numbers.
- You can search for IP ranges, including subnets. For example:
 - `172.168.1.1/24` or `172.168.1.1/255.255.255.0` matches all IP addresses in the subnet `172.168.1.1/255.255.255.0`
 - `172.168.1.1-140.255` matches all IP addresses from `172.168.1.1` to `172.168.140.255`
- You can search for URLs in multiple ways, using part or all of the URL. Searching for the full URL may not return enough results if the URL contains random substrings, such as session IDs. If your search keywords do not return enough results, try one of the following:
 - Full Search
 - shortening your keyword to the smallest necessary substring of the URL
 - shortening your keyword to a substring of the URL delimited by slash (/) characters
- The search returns results that match all, any, or none of the search terms, according to the option you select in Match.
For example, if you enter into Keyword(s):
`192.168.* action=login`
and if from Match you select All Words, log messages for attacks on `192.168.*` by `W32/Stration.DU@mm` do not appear in the search results, since although the first keyword (the IP address) appears in attack log messages, the second keyword (the name of the attack) does not appear, and so the match fails. If the match fails, the log message is not included in the search results.

Printing the search results

After completing a search, a Printable Version button appears, allowing you to download a printable HTML copy of the search results. You can print this file, or save it to your computer for later use.

To download the results, select Printable Version.

Downloading the search results

After completing a search, a Download Current View button appears, allowing you to download a log file reflecting the search results. Search results can be saved in comma-separated value (`.csv`) format or in standard log (`.log`) format.

To download log search results

- 1 Go to **Log > Search**.
- 2 Perform a search using either basic or advanced search.
If your search finds one or more matching log events, a Download Current View button appears next to the Printable Version button.
- 3 Select Download Current View.
Options appear for the download's file format and compression.
- 4 Configure the following:

Convert to CSV format	Downloads the log format as a comma-separated value (.csv) file instead of a standard .log file. Each log element is separated by a comma. CSV files can be viewed in spreadsheet applications.
Compress with gzip	Compress the .log or .csv file with gzip compression. For example, downloading a log formatted file with gzip compression would result in a download with the file extension .log.gz. Large logs require more time to download. Download times may be improved by selecting Compress with gzip.
- 5 Select OK.
- 6 If prompted by your web browser, select a location to save the file, or open it without saving.

Rolling and uploading logs

You can control device log file size and consumption of the FortiAnalyzer disk space by configuring log rolling and/or 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
- if the file size is not exceeded, checks to see if it is time to roll the log file. You configure the time to be either a daily or weekly occurrence, and when the roll occurs

When a log file reaches its maximum size, or reaches the scheduled time, the FortiAnalyzer unit saves the log files with an incremental number, and starts a new log file with the same name. For example, the current attack log is `alog.log`. Any subsequent saved logs appear as `alog.n.log`, where *n* is the number of rolled logs.

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.

To enable log rolling or uploading, go to **Log > Config**.

Figure 8: Device Log Settings

The screenshot shows the 'Device Log Settings' configuration window. It contains the following fields and options:

- Log file should not exceed: 100 MB
- Log file should be rolled: Optional (dropdown) even if size is not exceeded
- Enable log uploading
- Server type: FTP SFTP SCP
- Server IP address: 0.0.0.0
- Username: fortianalyzer-2
- Password: *****
- Confirm Password: *****
- Directory: uploaded_logs/2/
- Upload Files: When rolled Daily at 00:00
- Upload rolled files in gzipped format
- Delete files after uploading
- Apply button

Log file should not exceed

Enter the maximum size of each device log file. When the log file reaches the specified maximum size, the FortiAnalyzer unit saves the current log file with an incremental number and starts a new active log file. For example, if the maximum size is reached, the current `alog.log` is renamed to `alog.n.log`, then a new `alog.log` is created to receive new log messages.

Log file should be rolled... even if size is not exceeded

Set the time of day when the FortiAnalyzer unit renames the current log file and starts a new active log file.

- **Daily:** Roll log files daily, even if the log file has not yet reached maximum file size.
- **Weekly:** Roll log files weekly, even if the log file has not yet reached maximum file size.
- **Optional:** Roll log files only when the log file reaches the maximum file size, regardless of time interval.

Enable log uploading

Select to upload log files to an server when a log file rolls.

Server type

Select the protocol to use when uploading to a server:

- File Transfer Protocol (FTP)
- Secure File Transfer Protocol (SFTP)
- Secure Copy Protocol (SCP)

Server IP address

Enter the IP address of the log upload server.

Username

Enter the user name required to connect to the upload server.

Password

Enter the password required to connect to the upload server.

Confirm Password

Re-enter the password to verify correct entry.

Directory

Enter a location on the upload server where the log file should be saved.

Upload Log files

Select when the FortiAnalyzer unit should upload files to the server.

- **When rolled:** Uploads logs whenever the log file is rolled, based upon Log file should be rolled.
- **Daily at hh:mm:** Uploads logs at the configured time, regardless of when or what size it rolls at according to Log file should be rolled.

- Upload rolled files in gzipped format** Select to compress the log files in gzipped format before uploading to the server.
- Delete files after uploading** Select to remove the log file from the FortiAnalyzer hard disk after the FortiAnalyzer unit completes the upload.

Content Archive

Content archiving provides a method of simultaneously logging and archiving copies of content transmitted over your network, such as email and web pages.

FortiGate units can log metadata for common user content-oriented protocols. Content logs include information such as the senders, recipients, and the content of messages and files. If full content archiving is enabled, FortiGate units can also archive a copy of the associated file or message with the content log message. Both FortiGate content archive logs and their associated copies of files or messages can be stored and viewed remotely on a FortiAnalyzer unit, leveraging its large storage capacity for large media files that can be common with multimedia content. When content archives are received by the FortiAnalyzer unit, you can use data filtering similar to other log files to track and locate specific email or instant messages, or to examine the contents of archived files.

For more information about how to configure the FortiGate unit to send content archives to the FortiAnalyzer unit, see the [FortiGate Administration Guide](#).

This section includes the following topics:

- [Viewing content archives](#)
- [Customizing the content archive view](#)
- [Searching full email content archives](#)

Viewing content archives

The content viewer displays content archives of these types:

- HTTP web browsing (in Web Archive)
- email (in Email Archive)
- FTP transfer (in File Transfer)
- instant messaging (IM) conversations (in IM Chat)
- VoIP (in VoIP Archive)
- multi-media messages (in MMS Archive)

The content archive viewer can display full and/or summary content archives. Summary content archives are those which contain only a log message consisting of summary metadata. Full content archives are those which contain both the summary and a hyperlink to the associated archived file or message. For example, if the FortiAnalyzer unit has a full content archive for an email message, the Subject log field of email content archives contains a link that enables you to view that email message. If the FortiAnalyzer unit has only a content archive summary, the Subject field does not contain a link.

Whether or not each content archive will be full or summary varies by:

- whether the device is configured to send full content archives
- whether the content satisfies content archiving requirements

- whether the FortiAnalyzer unit has the copy of the file or message associated with the summary log message (that is, full content archives do not appear if you have deleted the associated copy of the file or message)

For more information about requirements and configuration of content archiving, see the [FortiGate Administration Guide](#).

To view content archives, go to **Content Archive**, then select the content archive type. Each type has similar controls.

Figure 1: Content Archive

#	Last Activity	Subtype	Source	URL
1	2007-03-27 15:41:19	HTTP	192.168.2.110	sb.google.com/safebrowsing/update?client=navclient-auto-ffox2.0
2	2007-03-27 15:39:00	HTTP	192.168.2.110	172.20.120.101/cgi-bin/unitaddr.cgi
3	2007-03-27 15:29:35	HTTP	192.168.2.110	sb.google.com/safebrowsing/update?client=navclient-auto-ffox2.0
4	2007-03-27 14:50:35	HTTP	192.168.2.110	www.bossus.com/podcasts/btr/btr_2007-03-23_03.mp3
5	2007-03-27 14:47:31	HTTP	192.168.2.110	podcast.cbc.ca/mp3/quirks_20070324_1921.mp3
6	2007-03-27 14:46:34	HTTP	192.168.2.110	www.bossus.com/podcasts/btr/btr_2007-03-23_02.mp3
7	2007-03-27 14:45:38	HTTP	192.168.2.110	podcast.cbc.ca/mp3/quirks_20070324_1920.mp3
8	2007-03-27 14:45:03	HTTP	192.168.2.110	wu.apple.com/tq/applewidgets/quote.asp?key=IHHisApplewidgTs&s
9	2007-03-27 14:44:50	HTTP	192.168.2.110	apple.accuweather.com/adcbn/apple/Apple_Weather_Data.asp?zjpc
10	2007-03-27 14:44:48	HTTP	192.168.2.110	wu.apple.com/tq/applewidgets/quote.asp?key=IHHisApplewidgTs&s

Show	Select the FortiGate device from the list.
Timeframe	Select the time span of log data that you want to view.
Resolve Host Name	Select to view the IP alias instead of the client's IP address. You must configure the IP aliases on the FortiAnalyzer unit for this setting to take effect. For more information, see "Configuring IP aliases" on page 61 . Note: This option is not available for the email content archive.
Formatted Raw	Select a view of the content log file. Selecting Formatted (the default) displays the content log messages in columnar format. Selecting Raw displays the content log messages as they appear in the content log files.
View per page	Select the number of rows of log entries to display per page.
Page <i>n</i> of <i>n</i>	Enter a page number, then press Enter to go to the page.
Column Settings	Select to change the columns to view and the order they appear on the page. For more information, see "Displaying and arranging log columns" on page 109 .
Search	Enter a keyword to perform a simple search on the available log information, then select Go or press the Enter key to begin the search. For more information about on search, see "Searching the logs" on page 101 .
Printable Version	Select to download an HTML file containing all content archive summaries that match the current filters. The HTML file is formatted to be printable. Time required to generate and download large reports varies by the total amount of log messages, the complexity of any search criteria, the specificity of your column filters, and the speed of your network connection.
Delete associated content archive files	Select to delete all content archive files associated with the currently selected device. Note: This option is not available for the VoIP content archive.



Note: Content Archive allows you to *both* view logged details and to download the archived files. If you want to display only the content archive log file, instead go to **Log > Browse** and select the device's `clog.log` file. For more information, see [“Log” on page 91](#).

By default, **Content Archive > MMS** is hidden. To display this content archive, see the `show_mms_archive` variable in the [FortiAnalyzer CLI Reference](#).

Customizing the content archive view

Log messages can be displayed in either Raw or Formatted view.

- Raw view displays log messages exactly as they appear in the log file.
- Formatted view displays log messages in a columnar format. Each log field in a log message appears in its own column, aligned with the same field in other log messages, for rapid visual comparison. When displaying log messages in Formatted view, you can customize the log view by hiding, displaying and arranging columns and/or by filtering columns, refining your view to include only those log messages and fields that you want to see.

To display logs in Raw or Formatted view

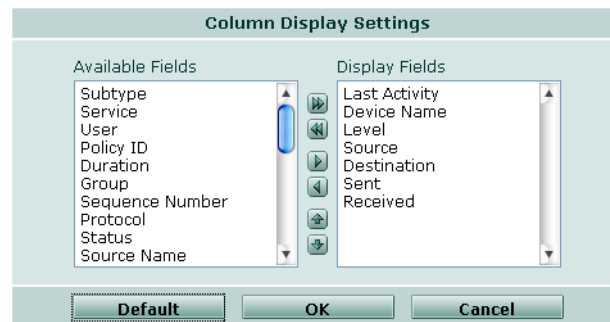
- 1 Go to a page which displays log messages, such as **Content Archive > Web Archive**.
- 2 Select Formatted or Raw.

Displaying and arranging log columns

When viewing logs in formatted view, you can display, hide and re-order columns to display only relevant categories of information in your preferred order.

For most columns, you can also filter data within the columns to include or exclude log messages which contain your specified text in that column. For more information, see [“Filtering logs” on page 110](#).

Figure 2: Customizing the column view



To display or hide columns

- 1 Go to a page which displays log messages, such as **Content Archive > Web Archive**.
- 2 Select Column Settings.

Lists of available and displayed columns for the log type appear.

- 3 Select which columns to hide or display.
 - In the Available Fields area, select the names of individual columns you want to display, then select the single right arrow to move them to the Display Fields area.
Alternatively, to display all columns, select the double right arrow.
 - In the Display Fields area, select the names of individual columns you want to hide, then select the single left arrow to move them to the Available Fields area.
Alternatively, to hide all columns, select the double left arrow.
 - To return all columns to their default displayed/hidden status, select Default.
- 4 Select OK.

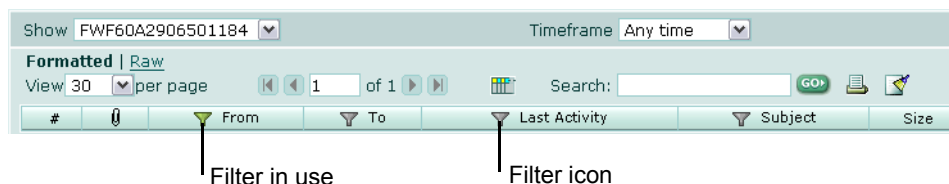
To change the order of the columns

- 1 Go to a page which displays log messages, such as **Content Archive > Web Archive**.
- 2 Select Column Settings.
Lists of available and displayed columns for the log type appear.
- 3 In the Display Fields area, select a column name whose order of appearance you want to change.
- 4 Select the up or down arrow to move the column in the ordered list.
Placing a column name towards the top of the Display Fields list will move the column to the left side of the Formatted log view.
- 5 Select OK.

Filtering logs

When viewing log messages, you can filter columns to display only those log messages that do or do not contain your specified content in that column. By default, most column headings contain a gray filter icon, which becomes green when a filter is configured and enabled.

Figure 3: Filter icons in the content logs



To filter log messages by column contents

- 1 In the heading of the column that you want to filter, select the filter icon.
- 2 Select Enable.
- 3 If you want to *exclude* log messages with matching content in this column, select NOT.
If you want to *include* log messages with matching content in this column, deselect NOT.

- 4 Enter the text that matching log messages must contain.
Matching log messages will be excluded or included in your view based upon whether you have selected or deselected NOT.
- 5 Select OK.
A column's filter icon is green when the filter is currently enabled.

To disable a filter

- 1 In the heading of the column whose filter you want to disable, select the filter icon.
A column's filter icon is green when the filter is currently enabled.
- 2 To disable the filter on this column, deselect Enable.
Alternatively, to disable the filters on all columns, select Clear All Filters. This disables the filter; it does not delete any filter text you might have configured.
- 3 Select OK.
A column's filter icon is gray when the filter is currently disabled.



Note: Filters do not appear in Raw view, or for unindexed log fields in Formatted view.

When viewing real-time logs, you cannot filter on the time column: by definition of the real-time aspect, only current logs are displayed.

Filtering tips

When filtering by source or destination IP, you can use the following in the filtering criteria:

- a single address (2.2.2.2)
- an address range using a wild card (1.2.2.*)
- an address range (1.2.2.1-1.2.2.100)

You can also use the Boolean operator "or" to indicate multiple alternative matches:

- 1.1.1.1 or 2.2.2.2
- 1.1.1.1 or 2.2.2.*
- 1.1.1.1 or 2.2.2.1-2.2.2.10

Most column filters require that you enter the column's entire contents to successfully match and filter contents; partial entries do not match the entire contents, and so will not create the intended column filter.

For example, if the column contains a source or destination IP address (such as 192.168.2.5), to create a column filter, enter the entire IP address to be matched. If you enter only one octet of the IP address, (such as 192) the filter will not completely match any of the full IP addresses, and so the resulting filter would omit all logs, rather than including those logs whose IP address contains that octet.

Exceptions to this rule include columns that contain multiple words or long strings of text, such as messages or URLs. In those cases, you may be able to filter the column using a substring of the text contained by the column, rather than the entire text contained by the column.

Searching full email content archives

You can search full email content archives to quickly locate and view messages, such as those whose body contains a specific term.

Full email content archive searches create a focused content archive view that contains only full content archives. Summary content archives are omitted.

To search full email content archives, go to **Content Archive > Email Archive > Search**.



Note: See “Searching the logs” on page 101 to search summary content archives.

Figure 4: Searching the email content archives

The screenshot shows a search interface with the following fields: From (empty), To (user1@example.com), Subject (empty), Message Contains (searc), Device (All Devices), and Date Within (Any time). A 'Search Archived Emails' button is present. Below the search fields is a pagination control showing 'View 30 per page' and '1 of 1'. The results table is as follows:

#	Attachment icon	From	To	Last Activity	Subject
1		exuser1@example.com	user1@example.com	2008-02-11 14:36:53	An example email content archive with attachment
2		exuser1@example.com	user1@example.com	2008-02-11 13:20:06	An example email content archive

Hyperlink to view archived email

- From** Enter all or part of the sender’s email address.
- To** Enter all or part of the recipient’s email address. For multiple recipients, enter any one of the recipients, or enter multiple recipient addresses in the order that they appear in the email address field, delimiting them with a comma (,) and a space, such as:
user1@example.com, user2@example.com
- Subject** Enter all or part of the subject line of the email.
- Message Contains** Enter all or part of a word or phrase in the email.
- Device** Select which device’s content archives to search.
- Date Within** Select a range of time to search.
- Search Archived Emails** Select to search full content archives using your specified search criteria. Search results appear below Date Within.
Only full content archives (that is, content archives that contain both a summary and a copy of the associated email message) will be searched. Summary content archives do not contain a copy of the email message, which is required to search the email message body, and therefore will not be searched.
- View n per page** Select the number of rows of search results to display per page.
- Page n of n** Enter a search result page number, then press Enter to go to that page.
- #** The index number of the search result.
- Attachment icon** If this column contains an attachment (paper clip) icon, the email contains an attachment.
- From** The sender’s email address.

To	The recipient's email address.
Last activity	The date and time that the FortiAnalyzer unit received the content archive.
Subject	The subject line of the email. Select the subject line of the email to view the email and its attachment, if any, in a pop-up window.
Size	The file size of the email, including any attachments.

Reports

FortiAnalyzer units can collate information collected from device log files and present the information in tabular and graphical reports, which provides quick analysis of what is occurring on the network.

By using reports, you can:

- minimize the effort required to identify attack patterns when customizing policies to prevent attacks
- monitor Internet surfing patterns for compliance with company policy
- identify your web site visitors for potential customers

FortiAnalyzer reports are also flexible, offering administrators a choice to compile a report layout based on variables (which can be reused) or based on specific information. Fortinet recommends a report layout based on variables and then reuse them.

This section includes the following topics:

- [Configuring reports](#)
- [Browsing reports](#)

Configuring reports

Logs must be collected or uploaded before you can generate a report. Logs are the basis of all FortiAnalyzer reports. After logs are collected or uploaded, you can then define the three basic components that make up a report:

- report layout (the layout and the contents)
- output and data filter templates, language (optional components)
- report schedule (log data parameters and time range)

You need to configure a report layout first, before configuring the report schedule because the report schedule requires a report layout. These output destination and data filter configurations are referred to as templates because they can be applied to any report layout or report schedule that you want.

If you are using data filter or output templates with a report schedule, these templates cannot be deleted. Data filter or output templates can be deleted when they are not being used by a report schedule.

When configuring a report layout, you can create individual charts that contain variables or specific log information, or both. You can configure multiple variable and specific charts within the report layout. The charts containing variables will always provide different information because they are not specific. The charts containing the specified information stay the same unless edited. Variable charts override specific charts.



















Note: Reports cannot be created for devices that are of an unknown type, such as generic Syslog devices, nor for devices that are not registered with the FortiAnalyzer unit's device list. For more information about on registering devices, see [“Manually adding a device” on page 80.](#)

Configuring report layout

The Layout tab enables you to configure and define multiple report layouts, which can then be applied to report schedules or generated immediately.

Figure 1: report layouts in Reports > Config > Layout

Create New		Delete			
<input type="checkbox"/>	Name	Description	Company Name	Number of Charts	
<input type="checkbox"/>	report_2			98	   
<input type="checkbox"/>	report_3			20	   
<input type="checkbox"/>	report_7			0	   
<input type="checkbox"/>	schedule_1			0	   

Delete
 Edit
 Clone
 Run Now

Create New

Select to create a new report layout and configure its settings.

Delete

Select to remove report layouts whose check boxes are selected.

- To delete one or more reports, select the check box next to their report name, then select Delete.
- To delete all reports, select the column heading check box. All reports' check boxes become select, and then select Delete.

You cannot delete report layouts that are currently being used in report schedules.

Report Name

The name of the report layout given when configuring a report layout.

Report Description

The description or comments entered in the Description field of the report layout.

Company

The name of the company, if given, when configuring the report layout.

Chart Number

The number of charts that are included in that report layout.

Action column

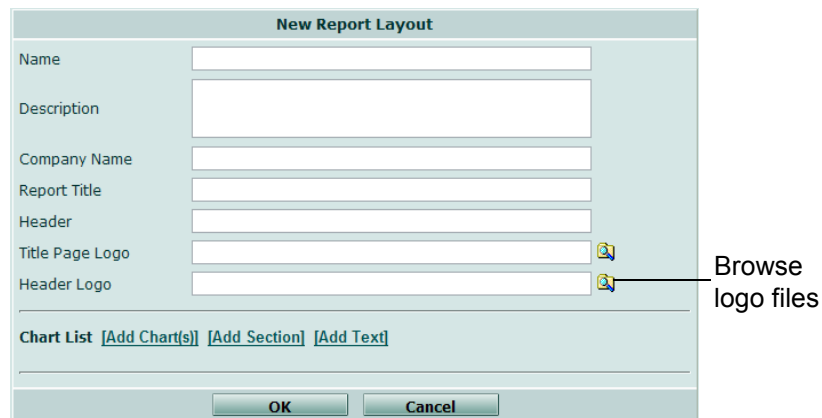
Select Edit to view or modify the report layout.

Select Clone to create a duplicate of a report layout to use as a basis for creating a new report layout.

Select Run Now to run a report layout immediately (on demand), instead of waiting for the report layout's scheduled time.

Select Delete to remove the report layout.

Figure 2: Layout



There are also default report layouts for you to choose from as well, and they appear in the report layout list with the report layouts you created. The default layouts are:

- Bandwidth_Analysis – is an overview of bandwidth consuming applications and users
- Threat_Analysis – is an overview of user Anti-Virus, Intrusion Protection and Anti-Spam threats for the time period
- Web_Filtering-Group_Activity – is an overview of user web site activity for a group of users while also providing a summary and analysis information on usage and behavior
- Web_Filtering-User_Activity – is an overview of user web site activity plus detailed audit of all blocked sites and all sites visited
- Forensic Analysis – is an overview of detailed network activity information such as instant messaging programs and email

When configuring a report layout, you can also choose and specify each individual chart. You can edit charts either during or after they are included in the report layout.

To configure a report layout

- 1 Go to **Report > Config > Layout**.
- 2 Select Create New.
- 3 Enter the appropriate information for the following:

Name	Enter a name for the report.
Description	Enter a description, for example, for what the report is about.
Company Name	Enter the name of your company or organization.
Report Title	Enter a title name for the report, for example, Report_1.

Title Page Logo Select the Browse logo files icon to choose a logo that will appear on the title page of the report. You need to select a logo file format that is compatible with your selected file format outputs. The logo will not appear if it is incompatible with the chosen file format.
You can choose JPG, PNG, and GIF logo formats for PDFs and HTMLS; WMF are also supported for RTF.

Header Logo Select the Browse logo files icon to choose a logo that will appear only in the header of the report. Logo formats for headers also need to be compatible with the chosen file format. The same logo formats for the title page also apply to headers.

4 Select [Add Chart(s)].

5 Enter the appropriate information for the following:

Device Type Select one of the device types from the drop-down list. The available types are FortiGate, FortiClient and FortiMail. The report's log information will come from the selected device type. For example, if you selected FortiMail, the log information used is only FortiMail logs. Note: Charts reflect what type of device you selected.

Category Select a category or all categories of charts from the drop-down list.

Chart Name Displays the name of each of the charts in each category. The category name is in bold, and the charts associated within that category name are displayed beneath.

Action Select the plus (+) symbol in the row containing the main chart name to add all charts of the category to the report.
Select the plus (+) symbol in each row to add charts individually.
When the plus (+) symbol is selected, a minus (-) symbol appears. Select the minus (-) symbol in each row to remove the selected chart or charts.

6 Select OK.

If you want to edit charts immediately after configuring them, go to the procedure ["To edit a chart" on page 117](#).

7 Select [Add Section].

8 Enter the appropriate information for the following:

Title Enter a title to describe the charts and information.

Description Enter a description, if applicable, to describe the charts.

9 Select OK.

10 Select [Add Text].

11 In the Message field, enter a sentence or paragraph to include a message at the bottom of the report.

12 Select OK.

If you want to rearrange the order of the charts, use your mouse to drag and drop each chart so that they are arranged in the order you want.



Note: Report layouts cannot be deleted if they are associated with a report schedule; if you want to delete a report layout, remove that layout from the schedule it is associated with, and then delete it.

Editing charts in a report layout

You can edit charts at any time as well as rearrange the charts from within the Chart List. You can also edit Text and Section as well. The following procedure assumes you have already selected the report layout that you want to edit charts, Text and Section in Layout.

To edit a chart

- 1 Select Edit beside the chart name.
- 2 Enter the appropriate information for the following:

Chart Output Select one of the following to display chart information:

- Table & Graph – displays both a table and graph
- Table – displays only a table
- Graph – displays only a graph

Chart Style Select a style for the chart. You can choose a bar style, column style or pie style.

Maximum Entries (Top N) Enter a number for the top ranked log information, such as top number of viruses, and if applicable, select the check box List All Results.

When entering a number for the maximum top entries (with pie chart style selected), any item whose percentage is less than one percent will not appear in the pie diagram; also, if no items' percentage is greater than one percent, "Other" occupies the pie diagram, or 100 percent of the pie diagram. For example, if you enter the number five, any of the five items that have less than one percent are considered under "Other" and only "Other" displays on the pie diagram.

This issue occurs only when the pie chart style is selected. The bar chart style is not affected.

Time Scale Select what type of time period you want the focus of the report to be on.

Advanced Select the following to specify the number and appearance of results in the report.

Resolve Host Names Select to display host name by an alias or reverse DNS lookup rather than IP addresses. For more information about on configuring IP aliases, see

Resolve Service Names Select to display network service names rather than port numbers such as HTTP instead of port 80.

Include "Other" Category (in graphs) Select to include the other results that are not included in the top entries, that display in a graph.

Override Run-time Variables Select to specify the following that will be associated with this chart.

Device Select to specify a device or device group from the drop-down list. You can also select all devices, if applicable.

User Enter the user's name that you want to use in the report. You can enter multiple names in the field, using commas to separate the user names.

- Group Enter a group's name that you want to use in the report. You can enter multiple names in the field, using commas to separate the group names.
- LDAP Query Select the LDAP Query check box and then select the LDAP directory or Windows Active Directory group from the drop-down list.
This is useful if you want to restrict report scope using a list of user names from the LDAP directory or Windows Active Directory group, instead of a group name configured on a device.

3 Select OK.

If you want to rearrange the charts so that they are presented in a different order, select and drag a chart (using your mouse) to above or below another chart. The order is reflected in the generated report.

To edit text

- 1 Select Edit beside the text name.
- 2 Clear the appropriate information that appears in the Message field.
- 3 Enter the new information in the Message field.
- 4 Select OK.

To edit section

- 1 Select Edit beside the section name.
- 2 Clear the appropriate information that appears in either Title or Description fields, or both fields.
- 3 Enter the new information in either Title or Description fields, or both fields.
- 4 Select OK.

Configuring report schedules

Report schedules are configured after you have configured report layouts. If you do not have a report layout, you cannot configure a report schedule.

When configuring report schedules, you can specify the variables selected for charts. Variables are only specified in report schedules.

Report schedules provide a way to schedule a daily, monthly or weekly report so that the report will generate at a specific time period. You can configure multiple report schedules in **Report > Schedule**.

Figure 3: Report schedules

Create New		Delete			
<input type="checkbox"/>	Schedule Name	Report Profile Name	Device	Schedule	
<input type="checkbox"/>	report1_scheduleA	report_1_branchoffice	FG100A2906500197	Daily: 11:00	
<input type="checkbox"/>	report_2_schedule	report_2_headquarters	All_FortiGates	Monthly: 17:00 at 1,10,30	
<input type="checkbox"/>	report_3A	report_2_headquarters	FG100A2906500197	Weekly: 18:00 at Wed	
<input type="checkbox"/>	test_report	report_2_headquarters	FG100A2906500197	Weekly: 12:00 at Wed,Thu	
<input type="checkbox"/>	test_schedule_2	report_2_headquarters	group_1_FGT60s	Monthly: 05:19 at 1,5,27	

Create New	Select to create a new report schedule and configure the settings.
Delete	Select to remove report schedules whose check boxes are selected. <ul style="list-style-type: none"> To delete one or more report schedules, select the check box next to their report name, then select Delete. To delete all reports, select the column heading check box. All report schedules' check boxes are selected, and then select Delete.
Schedule Name	The name given to the report schedule when configuring the report schedule.
report layout Name	The name of the report layout that is associated with the report schedule.
Device	The device or device group that is associated with the report schedule.
Schedule	The time period or range for the report, in the following formats: <ul style="list-style-type: none"> Daily: hh:mm Weekly: hh:mm at [days of week] Monthly: hh:mm at [dates of month]
Action	Select Delete to remove the report layout. Select Edit to view or modify the report schedule. Select Run Now to run a report schedule immediately, (on demand), instead of waiting for the scheduled time.



Caution: When configuring a report schedule, which contains both an output template and selected file formats in Output Types, the file formats sent by email are determined by the configuration settings. Only those file formats that are enabled in both output template and schedule output types are sent by email. For example, if PDF and Text formats are selected in the output template, and then PDF and MHT are selected in the report schedule, the report's file format in the email attachment is PDF.

To configure a report schedule

- 1 Go to **Report > Schedule**.
- 2 Select Create New.
- 3 Enter the appropriate information for the following:

Name	Enter a name for the schedule.						
Description	Enter a description for the schedule. This is optional.						
Layout	Select a configure report layout from the drop-down list. You must apply a report layout to a report schedule.						
Language	Select a language from the drop-down list or choose Default to use the default language.						
Schedule	Select one of the following to have the report generate only once, daily, weekly, or monthly at a specified date or time period. <table> <tr> <td>Once</td> <td>Select to have the report generated only once.</td> </tr> <tr> <td>Daily</td> <td>Select to generate the report every date at the same time. Enter the hour and minute time period for the report. The format is hh:mm.</td> </tr> <tr> <td>Weekly</td> <td>Select to generate the report on specified days of the week. Select the days of the week check boxes.</td> </tr> </table>	Once	Select to have the report generated only once.	Daily	Select to generate the report every date at the same time. Enter the hour and minute time period for the report. The format is hh:mm.	Weekly	Select to generate the report on specified days of the week. Select the days of the week check boxes.
Once	Select to have the report generated only once.						
Daily	Select to generate the report every date at the same time. Enter the hour and minute time period for the report. The format is hh:mm.						
Weekly	Select to generate the report on specified days of the week. Select the days of the week check boxes.						

	Monthly	Select to generate the report on a specific day or days of the month. Enter the days with a comma to separate the days. For example, you want to generate the report on the first day, the 21st day and 30th day: 1, 21, 30.
Log Data Filtering		<p>You can specify the variables that were selected in the charts when configuring the report layout.</p> <p>If you did not specify any variables in the charts added to report layout, proceed to Data Filter.</p> <p>Device/Group Select a device or device group from the list.</p> <p>Virtual Domain Select to create a report based on virtual domains. Enter a specific virtual domain to include in the report.</p> <p>User Select to create a report based on a network user. Enter the user or users in the field.</p> <p>Group Select to create a report based on a group network users, defined locally. Enter the name of the group or groups in the field.</p> <p>LDAP Query Select the LDAP Query check box and then select an LDAP directory or Windows Active Directory group from the drop-down list.</p>
Data Filter		Select a data filter template from the drop-down list to the report schedule.
Time Period	Local time for:	<p>Select to base the time period on the local time of the FortiAnalyzer unit or the selected devices. Log time stamps reflect when the FortiAnalyzer unit received the message, not when the device generated the log message. If you have devices located in different time zones, and are creating a report layout based on a span of time, ensure that the time span is relative to the device, not the FortiAnalyzer unit.</p> <p>For example, if you have a device and a FortiAnalyzer unit located three time zones apart, a report for the time frame from 9 AM to 11 AM will yield different results depending on whether the report time frame is relative to the device's local time, or to the FortiAnalyzer unit's local time.</p> <p>From: Select the beginning date and time of the log time range.</p> <p>To: Select the ending date and time of the log time range.</p>
Output		<p>Select the type of output you want the report to be in and if you want to apply an output template as well.</p> <p>Output Types Select the type of file format you want the generated report to be. You can choose from PDF, HTML (default), MS Word, Text, and MHT. Note: Only those file formats that are enabled in both output template and schedule output types are sent by email. For example, if PDF and Text formats are selected in the output template, and then PDF and MHT are selected in the report schedule, the report's file format in the email attachment is PDF.</p> <p>Email/Upload Select the check box if you want to apply a report output template from the drop-down list.</p>

4 Select OK.

Configuring data filter templates

You can configure multiple data filter templates for reports in **Report > Config > Data Filter**. These templates can be applied to any report schedule you want.

Figure 4: Data filter templates

<input type="checkbox"/> Create New		<input type="checkbox"/> Delete	
<input type="checkbox"/>	Name	Description	
<input type="checkbox"/>	datafilter_1		
<input type="checkbox"/>	datafilter_2		
<input type="checkbox"/>	datafilter_3	web activity	
<input type="checkbox"/>	datafilter_4	for branch office only	

Create New Select to create a new data filter template and configure its settings.

Delete Select to remove data filter templates whose check boxes are selected.

- To delete one or more data filter templates, select the check box next to their name, then select Delete.
- To delete all reports, select the column heading check box. All data filter templates' check boxes become selected, and then select Delete.

You cannot delete a data filter template if it is already being used by a report layout or report schedule. If you want to delete a data filter template that is being used by a report schedule, edit that report layout or report schedule to unselect the data filter template.

Name Displays the name of the data filter template

Description Displays any comments entered in the Description field when configuring the data filter template.

Action Select Delete to remove the data filter template.

Select Edit to view or modify the data filter template.

Data filters are configured to sort through and omit specific log information, enabling you to include or exclude log messages to focus your report on certain types of log messages that match your criteria. For example, you want to include a specific range of IP addresses. In the Source(s) field you input the IP addresses range, 172.20.110.0-255, which will match all IP addresses in the 172.20.110.0/255.255.255.0 or 172.20.120.110/24. If you do not want to match this specific IP address range, you would enter the IP address range and select the “not” check box.

Data filter options operate on specific log message fields. For information about log message fields, see the *FortiGate Log Message Reference*.

Figure 5: Configuring a data filter template

The screenshot shows the 'New Data Filter' configuration window. It has several sections:

- Name:** A text input field.
- Description:** A larger text input field.
- Filter Logic:** Radio buttons for 'all' (selected) and 'any'.
- Source(s):** Text input with an 'Alias' dropdown and a 'not' checkbox.
- Destination(s):** Text input with an 'Alias' dropdown and a 'not' checkbox.
- Interface(s):** Text input with a 'not' checkbox.
- Policy ID(s):** Text input with a 'not' checkbox.
- Service(s):** Text input with a 'not' checkbox.
- Day of Week:** Checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, Sat.
- Web Category:** A dropdown menu labeled 'Web Category' and a 'Category List' with checkboxes for: Potentially Liable, Objectionable or Controversial, Potentially Non-productive, Potentially Bandwidth Consuming, Potentially Security Violating, General Interest, Business Oriented, and Others.
- Priority:** Two list boxes: 'Available Levels' (Emergency, Alert, Critical, Error, Warning, Notification, Information) and 'Selected Levels'.
- Generic Filter(s):** A 'Key:' and 'Value:' input pair with a 'not' checkbox, and a large text area below.
- Buttons:** 'Add' and 'Delete' buttons at the bottom right.

To configure data filters for a report

- 1 Go to **Report > Config > Data Filter**.
- 2 Select Create New.
- 3 Enter and/or select the appropriate information for the fields and check boxes for the following:

- Name** Enter a name for the new data filter configuration. This name only concerns this particular data filter configuration, not the report itself.
- Description** Enter a description for the report. This is optional.
- Filter logic** Select "all" to include only logs in the report that match all filter criteria. If any aspect of a log message does not match all criteria, the FortiAnalyzer unit will exclude the log message from the report.

Select "any" to include logs in the report that match any of the filter criteria. If any aspect of a log message matches any of the filter criteria, the FortiAnalyzer unit will include the log in the report.
- Source(s)** Enter the source or sources of IP addresses to include matching logs. You can also select from the alias list. Separate multiple sources with a comma.

Alias	Select the appropriate alias from the drop-down list. See Configuring IP alias on page 50 for more information about configuring IP aliases. You can filter on IP ranges or subnets. For example: <ul style="list-style-type: none"> • 172.20.110.0-255 matches all IP addresses in the 172.20.110.0/255.255.255.0 or 172.20.120.110/24 • 172.20.110.0-140.255 matches all IP addresses from 172.20.110.0 to 172.20.140.255 • 172.16.0.0-20.255.255 matches all IP addresses from 172.16.0 to 172.20.255.255
not	Select to instead include only log messages that do not match this criterion. For example, you might include logs except those matching a specific source IP address.
Destination(s)	Enter the destination IP address to include matching logs, or select from the Alias list. Separate multiple sources with a comma. See “Configuring IP aliases” on page 61 for more information about configuring IP aliases.
Alias	Select the appropriate alias. Select the appropriate alias from the drop-down list. See Configuring IP alias on page 50 for more information about configuring IP aliases. You can filter on IP ranges or subnets. For example: <ul style="list-style-type: none"> • 172.20.110.0-255 matches all IP addresses in the 172.20.110.0/255.255.255.0 or 172.20.120.110/24 • 172.20.110.0-140.255 matches all IP addresses from 172.20.110.0 to 172.20.140.255 • 172.16.0.0-20.255.255 matches all IP addresses from 172.16.0 to 172.20.255.255
not	Select to instead include only log messages that do not match this criterion. For example, you might include logs except those matching a specific destination IP address.
Interface(s)	Enter the network interface or interfaces to include matching logs. Separate multiple interface names with a comma
not	Select “not” to instead include only log messages that do not match this criterion. For example, you might include logs except those matching a specific network interface.
Policy ID(s)	Enter the FortiGate firewall Policy ID numbers to include matching logs. The report will include logs from all FortiGate log files containing firewall policy ID numbers, which excludes event and content archive logs. Separate multiple policy IDs with a comma.
not	Select to instead include only log messages that do not match this criterion. For example, you might include logs except those matching a specific policy ID.
Service(s)	Enter specific services to include matching logs. Separate multiple services with a comma.
not	Select “not” to instead include only log messages that do not match this criterion. For example, you might include logs except those matching a specific service.
Day of the Week	Select specific days of the week to include matching logs.

- Web Category Category List** Select the categories you want to filter logs by selectively including web filtering logs that match your criteria, then indicate included categories by selecting one or more category check box. Select "not" to instead include only logs that do not match the criterion.
- You can select a whole category by selecting the check box beside the blue arrow of the category. You can also select the individual sub-categories that are within the category by selecting the blue arrow to display the sub-categories. For example, you might select to include all web filtering logs with a category of "Potentially Bandwidth Consuming", or you might select only "Internet Radio and TV" within that category.
- Priority** Select a severity level from the Available Levels column and then use the -> arrow to move the level to the Selected Levels column. If you want to remove a severity level from the Selected Levels column, select the level first and then use the <- arrow to move the level back to the Available Levels column.
- Generic Filter(s)** Enter a generic filter for the filter template.
- Key Enter a keyword in this field.
 - Value Enter a number for the value. Select the "not" check box to instead include only log messages that do not match the generic filter criteria.
 - Add Select Add to add the keyword and value number to the generic filter list. The generic filter list displays all configured generic filters in the field beside both Add and Delete.
 - Delete Select to delete the generic filter. Select the generic filter first, and then select Delete.

4 Select OK.

Configuring report output templates

You can configure the FortiAnalyzer unit to output the report in one or more file formats, save the reports of selected file formats to the FortiAnalyzer hard disk, and email the report to recipients. You can make multiple report output templates and assign them to different report schedules.

Figure 6: Output templates

<input type="checkbox"/>	Name	E-Mail Destination	FTP/SFTP/SCP Server IP	
<input type="checkbox"/>	output_1	aa@example.com(from bb@example.com through mail.example.com)		
<input type="checkbox"/>	output_2	hh@example.com(from gg@example.com through mail.example.com)	10.10.16.155(FTP)	

- Create New** Select to create a new report output template.
- Delete** Select to remove report output templates whose check boxes are selected.
- To delete one or more report output templates, select the check box next to their name, and then select Delete.
 - To delete all reports, select the column heading check box. All templates' check boxes are selected, and then select Delete.
- You cannot delete a report output template if it is being used by a report layout or report schedule. If you want to delete a report output template that is being used by a report layout or report schedule, edit that report layout or report schedule to unselect the data filter template.
- Output Name** The name of the output template.

- E-Mail Destination** The route the email will take when sent, in the format, <recipient_email address> (from <sender_email address> through <email server>).
- FTP/SFTP/SCP Server IP** The type of server that the report will be uploaded to in the format, <ipv4>(typeofserver). For example, 10.10.20.15(FTP).
- Action** Select Edit to view or modify the report output.
Select Delete to remove the report output.

When configuring the FortiAnalyzer unit to email a report, you must first configure the FortiAnalyzer unit to connect to an email server. For more information, see [“Configuring alerts by email server” on page 135](#).

If HTML reports are sent to a user that has an email client without supported HTML, the HTML code for the reports will display in the message body.

You cannot delete a report output configuration if it is already being used in another report.

Figure 7: Output template

To configure the output for a report

- 1 Go to **Report > Config > Output**.
- 2 Select Create New.
- 3 Enter and/or select the appropriate information for the fields and check boxes for the following:

- Name** Enter a name for the report. This name only concerns the report output configuration that you are configuring for your report., not the report itself.
- Description** Enter a description for the report. This is optional.

Send Report by Mail	Verify this check box is selected. If you do not want to send a report by email, unselect the check box. If the check box is unselected, the available options under Send Report by Mail are hidden.				
Email Output	<p>If you want to email the report as an email attachment, select one or more of the following file formats:</p> <ul style="list-style-type: none"> • HTML (default) • PDF • MS Word (RTF) • Text (ASCII) • Multi-purpose Internet Mail Extension HTML format (MHT) • Compress Report Files <p>You need to also configure the required email fields to complete the configuration, such as Email subject, Email Body, Email To, and Email Server.</p> <p>If you select the Compress Report Files check box, the report files will be compressed into a .zip file and that .zip file is attached to the email.</p> <p>Note: Only those file formats that are enabled in both output template and schedule output types are sent by email. For example, if PDF and Text formats are selected in the output template, and then PDF and MHT are selected in the report schedule, the report's file format in the email attachment is PDF.</p>				
Email Attachment Name	<p>Select Use Default if you want the attached report name to be the name given of the report when configuring the layout in Layout.</p> <p>Select Specify to enter a specific name for the attached report in the field. This name will appear as the attachment's name, and is not the report's actual name.</p>				
Email From	Enter a sender email address for the FortiAnalyzer unit or administrator configure the report.				
Email Server	Select which email server to use when the FortiAnalyzer unit sends reports as an email, or select Create New to configure a new email server connection.				
Email To	Enter the email addresses of the recipients of the report. Add multiple recipients by selecting Add after each email address. These email addresses display in the email list.				
Email List	<p>Displays email addresses in the format, <recipient_email address> (from <sender_email address> through <email server>).</p> <p>If you want to remove an email address from the list, select the email address you want removed, and then select Delete.</p>				
Email Subject	Enter a subject for the report email. If you do not enter a subject, the subject line will be the name of the report.				
Email Body	Enter text to include in the body of the email message.				
Upload Report to FTP Server	<p>Select to upload completed report files to a server accepting FTP, SFTP, or SCP. These options are only available when the Upload Report to FTP Server check box is selected.</p> <p>Note: When sending reports to an FTP server, the following are sent: HTML, PDF and MHT.</p> <table border="0" style="width: 100%;"> <tr> <td style="vertical-align: top;">Server Type</td> <td>Select the protocol to use when connecting to the upload server. Select from: <ul style="list-style-type: none"> • File Transfer Protocol (FTP) • Secure File Transfer Protocol (SFTP) • Secure Copy Protocol (SCP) </td> </tr> <tr> <td style="vertical-align: top;">IP Address</td> <td>Enter the IP address of the upload server.</td> </tr> </table>	Server Type	Select the protocol to use when connecting to the upload server. Select from: <ul style="list-style-type: none"> • File Transfer Protocol (FTP) • Secure File Transfer Protocol (SFTP) • Secure Copy Protocol (SCP) 	IP Address	Enter the IP address of the upload server.
Server Type	Select the protocol to use when connecting to the upload server. Select from: <ul style="list-style-type: none"> • File Transfer Protocol (FTP) • Secure File Transfer Protocol (SFTP) • Secure Copy Protocol (SCP) 				
IP Address	Enter the IP address of the upload server.				

Username	Enter the user name the FortiAnalyzer unit will use when connecting to the upload server.
Password	Enter the password the FortiAnalyzer unit will use when connecting to the upload server.
Directory	Enter the directory path that the FortiAnalyzer unit will upload the report to.
Upload report(s) in gzipped format	Select to compress the report files using gzip format before uploading to the server.
Delete file(s) after uploading	Select to delete the report files from the FortiAnalyzer hard disk after the FortiAnalyzer unit has completed uploading the report files to the server.

4 Select OK.

Configuring language

When creating a report layout, you can select which language the report will be written in. If your preferred languages require modification, you can create your own report language customization, which then becomes available for selection in the report layout.

Report language components include:

- a string file, also known as a language resource file, containing report text
- a format file specifying the language encoding, as well as file format specific settings
- a font file whose glyphs support your encoding's character set

The font file is used to render graph titles and Y-axis labels in a font of your choice. Some fonts, particularly for double-byte languages, do not support character rotation, which is required by the Y-axis label. Compatible fonts must be a TrueType (.ttf) font, and must support character rotation. Examples of known compatible fonts include Arial, AR PL Mingti2L Big5, AR PL SungtiL GB, DFPHSGothic-W5, and Verdana.

The string file specifies pieces of text that may be used in various places throughout the report. Each string line consists of a key followed by an equal symbol (=) and its value. You can add comments to the string file by preceding them with a number symbol (#).

For example, in these lines:

```
# Printed in place of report when zero log messages
  matched report filter.

no_match=No matching log data for this report
```

the comment is:

```
# Printed in place of report when zero log messages
  matched report filter.
```

the key is `no_match`, and the string value for that key is `No matching log data for this report`.

Keys are required and must not be removed or changed. Keys map a string to a location in the report, and are the same in each language file. If you change or remove keys, the FortiAnalyzer unit cannot associate your string with a location in the report, string file validation will fail, and the string file upload will not succeed.

String values may be changed to customize report text. If your custom string values use a different encoding or character set than the default language file, customize your format file to reflect your new character set and/or encoding.

Comment lines are optional; you can add them throughout the file to provide notes on your work.

The format file contains settings for the file format renderers, including encodings. The format file contains sections that are preceded by an output type label, consisting of the file format name followed by a colon character (:). Within each output type's section, one or more settings exist, consisting of a variable name followed by an equal symbol (=) and its value, contained by quote characters (""). You can add comments to the format file by preceding them with a number symbol (#).

For example, in these lines:

```
# Localization uses a Latin character set.
html:
html_charset="iso-8859-1"
```

The comment is:

```
# Localization uses a Latin character set.
```

The output type label is `html:`, the variable name is `html_charset`, and the variable's value is `iso-8859-1`.

Variables are required and must not be removed or changed. If you change or remove variables, the FortiAnalyzer unit may not be able to properly format your reports.

If your custom string values use a different encoding or character set than the default language file, you must customize your format file to reflect your new character set and/or encoding. If your string file requires double-byte encoding, also set `doublebytes="1"`. Otherwise, set `doublebytes="0"`. The variable's value must be in a pattern acceptable by the output type. If variable value syntax is not correct, format file validation will fail, and the format file upload will not succeed.

Supported encodings used by the string file and referenced in the format file include those specified by the PDF, RTF, and HTML standards. For character set and encoding syntax and other specifications, see:

- [W3C HTML 4.01 Specification](#)
- [Adobe PDF Reference](#)
- [Microsoft Word 2003 Rich Text Format \(RTF\) Specification, version 1.8](#)

Comment lines are optional; you can add them throughout the file to provide notes on your work.

If you require further format file customization, including adjustments to PDF objects, contact Fortinet Technical Support.



Note: Both format and string files use Unix-style line endings (LF characters, not CR-LF).

Figure 8: Languages

Create New			
Language	Description	Font	Action
English	English		
Japanese	Japanese		
SampleLang	A sample language customization.	Arial	
Simplified_Chinese	Simplified Chinese		
Spanish	Spanish		
Traditional_Chinese	Traditional Chinese		

Delete
 Edit
 Download Format File
 Download String File
 Download Font File

Create New	Select to create a new report language customization.
Language	The name of the report language customization.
Description	The description of the report language customization.
Font	If you uploaded a font file with your report language customization, the name of the font. This does not appear if the report language uses a default font.
Action	Select Delete to remove a report language customization. This option does not appear for default report languages. Select Download Format File to download the file format settings. Select Download String File to download the language resource. Select Download Font File to download the custom font file. This option does not appear for default languages and report language customizations using a default font.

To create a report language customization

- 1 Go to **Report > Config > Language**.
- 2 Locate the default language that you want to customize. In that language's row, select Download Format File and Download String File from the Action column.
- 3 Open the string file using a plain text editor that supports Unix-style line endings and the string file's encoding, such as [jEdit](#). Verify that the correct encoding has been detected or selected.
- 4 Locate and edit text that you want to customize.
Do not change or remove keys. Modifiable text is located to the right of the equal symbol (=) in each line.
- 5 Save the string file.

- 6 If you changed the encoding of the string file, open the format file using a plain text editor that supports Unix-style line endings, such as [jEdit](#), and edit the encoding and character set values for each file format. If you have switched between a single-byte and a double-byte encoding, also set the `doublebytes` value to true (1) or false (0).

For specifications on how to indicate encoding and character set, refer to each file format's specifications:

- [W3C HTML 4.01 Specification](#)
- [Adobe PDF Reference](#)
- [Microsoft Word 2003 Rich Text Format \(RTF\) Specification, version 1.8](#)

- 7 Save the format file.
- 8 Go to **Report > Config > Language**.
- 9 Select Create New to create a separate language option, or select Edit in the Action column of a language's row to replace an existing language.
- 10 If you are creating a new report language, enter the Language of the report. The Language name cannot contain spaces.
- 11 Enter a Description for the language.
- 12 For the Format File, select Browse and locate your customized format file.
- 13 For the String File, select Browse and locate your customized string file.
- 14 If you want to customize the font of report graph titles and Y-axis labels, for Font File, select Browse and locate your font.

If your font is located in the system font folder, you may need to first copy the font from the system font folder to another location, such as a temporary folder or your desktop, to be able to select the font for upload.



Note: Some font licenses prohibit copying or simultaneous use on multiple hosts or by multiple users. Verify your font's license.

- 15 Select OK.
- Time required to upload the language customization files varies by the size of the files and the speed of your connection. If there are any errors with your files, correct the errors, then return to step 8.

Table 9: Language file error messages

Error message	Description
Specified format file contains invalid syntax.	Your format or string file contains syntax errors. To locate the errors, compare your customized file with a default language's file. Refer to file format specifications or view default files for valid syntax.
Specified language string file is missing one or more strings.	Your string file is missing strings for one or more keys. To locate missing strings, compare your customized format file with a default language's string file.
Specified font file is not a standard TrueType font (*.ttf).	Your font file is not a TrueType font. Only TrueType fonts are supported.

After successfully uploading and verifying, your custom language becomes available as a report output language.



Note: The string file contains many keys, and each report type uses a subset of those keys. If your language modification does not appear in your report, verify that you have modified the string of a key used by that report type.

To change a report language customization

- 1 Go to **Report > Config > Language**.
- 2 Locate the customized language whose font, string, or format file you want to change and in that language's row, select Edit from the Action column.
- 3 For the string, format, and/or font file, select Browse and locate the replacement file(s).

If you have previously provided a custom font file, you can replace it, but cannot remove the font file.

- 4 Select OK.

Time required to upload the language customization files varies by the size of the files and the speed of your connection. If there are any errors with your files, correct the errors, then return to step 3.

After successfully uploading and verifying, your custom language becomes available as a report output language.

To delete a report language customization

- 1 Go to **Report > Config > Language**.
- 2 Locate the customized language that you want to remove. In that language's row, select Delete from the Action column.

A confirmation message appears.

- 3 Select OK.

Browsing reports

After reports are generated by the FortiAnalyzer unit, you can view them in **Report > Browse > Result**. The Report Result page displays all generated reports, including generated scheduled reports.

Figure 9: Viewing reports in Report > Browse

Refresh		Delete		Device Type: All_Device		1 of 40			
<input type="checkbox"/>	Report Files	Device Type	Started	Finished	Size (bytes)	Other Formats	Action		
<input type="checkbox"/>	▶ Scheduled_test_report-2008-06-05-1200	FortiGate	Thu Jun 5 12:00:01 2008	Thu Jun 5 12:00:08 2008		PDF			
<input type="checkbox"/>	▶ Scheduled_report1_scheduleA-2008-06-05-1100	FortiGate	Thu Jun 5 11:00:01 2008	Thu Jun 5 11:00:12 2008		PDF			
<input type="checkbox"/>	▶ Scheduled_test_schedule_2-2008-06-05-0519	FortiGate	Thu Jun 5 05:19:00 2008	Thu Jun 5 05:19:06 2008		MS Word PDF			
<input type="checkbox"/>	▶ Scheduled_report_3A-2008-06-04-1800	FortiGate	Wed Jun 4 18:00:00 2008	Wed Jun 4 18:00:06 2008		PDF Text			
<input type="checkbox"/>	▶ Scheduled_test_report-2008-06-04-1200	FortiGate	Wed Jun 4 12:00:00 2008	Wed Jun 4 12:00:06 2008		PDF			
<input type="checkbox"/>	▶ Scheduled_report1_scheduleA-2008-06-04-1100	FortiGate	Wed Jun 4 11:00:00 2008	Wed Jun 4 11:00:07 2008		PDF			
<input type="checkbox"/>	▶ Scheduled_report1_scheduleA-2008-06-03-1100	FortiGate	Tue Jun 3 11:00:01 2008	Tue Jun 3 11:00:06 2008		PDF			
<input type="checkbox"/>	▶ Scheduled_report1_scheduleA-2008-06-02-1100	FortiGate	Mon Jun 2 11:00:00 2008	Mon Jun 2 11:00:11 2008		PDF			
<input type="checkbox"/>	▶ Scheduled_sampleFCTReport-2007-07-12-1430	FortiClient	Thu Jul 12 11:30:00 2007	Thu Jul 12 11:30:16 2007					
<input type="checkbox"/>	▶ Scheduled_sampleFCTReport-2007-07-14-1430	FortiClient	Sat Jul 14 11:30:01 2007	Sat Jul 14 11:30:17 2007					
<input type="checkbox"/>	▶ Scheduled_sampleFCTReport-2007-07-15-1430	FortiClient	Sun Jul 15 11:30:02 2007	Sun Jul 15 11:30:18 2007					
<input type="checkbox"/>	▶ Scheduled_sampleFCTReport-2007-07-26-1430	FortiClient	Thu Jul 26 11:30:00 2007	Thu Jul 26 11:30:15 2007					
<input type="checkbox"/>	▶ Scheduled_sampleFCTReport-2007-08-03-1430	FortiClient	Fri Aug 3 11:30:00 2007	Fri Aug 3 11:30:17 2007					
<input type="checkbox"/>	▶ Scheduled_sampleFCTReport-2007-08-09-1430	FortiClient	Thu Aug 9 11:30:00 2007	Thu Aug 9 11:30:21 2007					
<input type="checkbox"/>	▶ Scheduled_sampleFCTReport-2007-08-20-1430	FortiClient	Mon Aug 20 11:30:00 2007	Mon Aug 20 11:30:18 2007					
<input type="checkbox"/>	▶ Scheduled_sampleFCTReport-2007-08-22-1430	FortiClient	Wed Aug 22 11:30:02 2007	Wed Aug 22 11:30:23 2007					
<input type="checkbox"/>	▶ Scheduled_sampleFCTReport-2007-08-30-1430	FortiClient	Thu Aug 30 11:30:01 2007	Thu Aug 30 11:30:24 2007					
<input type="checkbox"/>	▶ Scheduled_sampleFCTReport-2007-09-04-1430	FortiClient	Tue Sep 4 11:30:05 2007	Tue Sep 4 11:30:29 2007					
<input type="checkbox"/>	▶ Scheduled_sampleFCTReport-2007-09-10-1430	FortiClient	Mon Sep 10 11:30:01 2007	Mon Sep 10 11:30:41 2007					

- Refresh** Select to refresh the list. If the FortiAnalyzer unit is in the process of generating a report, use Refresh to update the status of the report generation.
- Delete** Select the reports from the listing by selecting the check box next to the report name.
- Device Type** Select the reports based on the type of device included in the report.
- Page Navigation** Enter a page number to display reports when a report list spans multiple pages. Select Go to move to the page.
Use the page forward and page back arrows to navigate through individual pages.
- Report Files** Select the report name to view the report in HTML format.
The report appears in the reports list with the report name, date and time the report was generated.
For example, a report name of "Report 1-2006-03-31-2112", is a report called "Report 1", generated on March 31, 2006 at 9:12 PM.
Select the blue arrow to expand the report to view the individual reports in HTML format.
- Started** The date and time when the FortiAnalyzer unit generated the report.
- Finished** The date and time when the FortiAnalyzer unit completed the report. If the FortiAnalyzer unit is in the process of generating a report, a progress bar will appear in this column. If the FortiAnalyzer unit has not yet started generating the report, which can occur when another report is not yet finished, Pending appears in this column.
- Size (bytes)** The file size of the report's HTML format output, if any.
The size does not reflect other output formats that may be present, such as PDF.
- Other Formats** Select a file format, if any, to view the generated report in that format.
In addition to HTML, if any, the generated reports may also be available in PDF, RTF and ASCII text formats, depending on the output configuration. For more information about setting output options, see "Configuring report output templates" on page 123.
- Action** Select Rename to rename the report. The icon to rename the report only appears after report generation has completed.
Select Delete to remove the report.



Quarantine

FortiAnalyzer units can act as a central repository for files that are suspicious or known to be infected by a virus, and have therefore been quarantined by your FortiGate units. This section describes how to view quarantined files.

If a secure connection has been established with the device, the communication between the two units is the same IPSec tunnel that the FortiGate unit uses when sending log files.

For more information about configuring the FortiGate unit to send quarantined files to the FortiAnalyzer unit, see the [FortiGate Administration Guide](#).

This section includes the following topics:

- [Viewing quarantined files](#)



Note: Sending quarantine files to a FortiAnalyzer unit is available only on FortiGate units running FortiOS 3.0 or later.

FortiAnalyzer units do not accept quarantine files from devices that are not registered within the FortiAnalyzer unit's device list. For more information about adding devices, see ["Manually adding a device" on page 80](#).

Viewing quarantined files

The quarantine repository displays a list of files quarantined by FortiGate units to the FortiAnalyzer hard disk.

To view quarantined files, go to **Quarantine > Repository**.

Figure 1: Viewing quarantined files

Show	Select a device from the list of available devices to display the list of quarantined files for a specific device.
Timeframe	Select a span of time when quarantined files were sent to the FortiAnalyzer unit and select Go.
Automatically Refresh	Select how often the quarantine page automatically updates. Select Refresh to update the status page immediately.
Delete	Select a file from the list by selecting the check box next to the name and select Delete to remove the quarantined file from the FortiAnalyzer hard disk.
Page <i>n</i> of <i>n</i>	Select a page number <i>x</i> from the list of pages <i>y</i> and press Enter to see the page.
View <i>n</i> per page	Select the number of quarantined files to view on a single page.
From Device	The name of the device where the quarantined file originated.
File Name	The processed file name of the quarantined file.

Date & Time	The date and time the FortiGate quarantined the file, in the format <code>yyy/mm/dd hh:mm:ss</code> . The time and date indicates the time that the first file was quarantined, if duplicate files are quarantined.
Service	The service by which the quarantined file was attempting to be transmitted, such as SMTP.
Checksum	A 32-bit checksum the FortiGate unit created from the file.
Status Description	A short description of the reason why the FortiGate unit quarantined the file.
DC	Duplicate count. A count of how many duplicates of the same file were quarantined. A rapidly increasing number can indicate a virus outbreak.
Size (Bytes)	The file size of the quarantined file.
Action	Select Delete to remove the quarantined file from the FortiAnalyzer hard disk. Select Detail to view more information about the file, including the date and time of the quarantine and the sender and intended recipient of the file. Select Download to save the file to another location when it is deemed safe for the recipient to collect. Caution: Quarantined files are suspected or known to contain a virus or other network threat. Inspecting quarantine files involves a significant security risk. Use caution when downloading quarantined files.

Alert

Alerts provide a method of informing you of issues arising on a FortiGate unit, FortiClient installation, or the FortiAnalyzer unit itself, such as system failures or network attacks, enabling you to react in a timely manner to the event.

You can configure the FortiAnalyzer unit alert conditions, instructing the FortiAnalyzer unit what devices and what log messages to monitor, and what to do in the event a log message appears meeting the alert conditions.

This section includes the following topics:

- [Alert Events](#)
- [Output](#)

Alert Events

Alert events define log message types, severities and sources which trigger administrator notification. For example, you could configure a trigger on the attack logs with an SMTP server output if you want to receive an alert by email when your network detects an attack attempt.

You can choose to notify administrators by email, SNMP or Syslog, as well as the Alert Console Messages section of the Dashboard. For more information on viewing alerts locally, see [“Viewing alert console messages” on page 34](#).

To view configured alert events, go to **Alert > Alert Event**.

Figure 1: Alert events list

		Create New	Delete			
<input type="checkbox"/>	#	Name	Devices	Triggers	Destination	Action
<input type="checkbox"/>	1	pri1	FGT5002801021077	Attack Log,AV Log	from faz1@example.com to admin@example.com through example.com	
<input type="checkbox"/>	2	tFortiClient	All_FortiClients	Event Log,Attack Log,AV Log,Webfilter Log	SYSLOG Server:cPC	

Delete |
Edit |

Create New	Select to add a new alert event.
Delete	Select to remove multiple alert events from the table. To do this, select the check box next to the alert events and select Delete.
Name	The name given to the alert event.
Devices	The devices the FortiAnalyzer unit is monitoring for the alert event.
Triggers	The log message packets the FortiAnalyzer unit is monitoring for the alert event.
Destination	The location where the FortiAnalyzer unit sends the alert message. This can be an email address, SNMP Trap or syslog server.
Action	Select Delete to remove the alert event. Select Edit to change the alert event configuration.

Adding an alert event

Adding an alert event enables you to receive notification when certain types of log messages are received.

To add a new alert event

- 1 Go to **Alert > Alert Event**.
- 2 Select **Create New**.
- 3 Configure the following options:

Alert Name	Enter a name indicating the type of alert the FortiAnalyzer is monitoring for.
Device Selection	Select the devices the FortiAnalyzer unit monitors for the alert event. Select from the Available Devices list and select the right arrow to move the device name to the Selected Devices list. Hold the SHIFT or CTRL keys while selecting to select multiple devices.
Trigger(s)	Select the triggers that the FortiAnalyzer unit uses to indicate when to send an alert message. Select the following: <ul style="list-style-type: none"> • a log type to monitor, such as Event Log or Attack Log • the severity level to monitor for within the log messages, such as >= • the severity of the log message to match, such as Critical <p>For example, selecting Event Log >= Warning, the FortiAnalyzer unit will send alerts when an event log message has a level of Warning, Error, Critical, Alert and Emergency.</p> <p>These options are used in conjunction with Generic Text and Device Selection to specify which log messages will trigger the FortiAnalyzer unit to send an alert message.</p>
Log Filters (Generic Text)	Select the check box Generic Text to enable log filters, and then enter log message filter text. This text is used in conjunction with Trigger(s) and Device Selection to specify which log messages will trigger the FortiAnalyzer unit to send an alert message. Enter an entire word, which is delimited by spaces, as it appears in the log messages that you want to match. Inexact or incomplete words or phrases may not match. For example, entering <code>log id</code> or <code>log it</code> may not match; entering <code>log id=0100000075</code> will match all log messages containing that whole word. Do not use special characters, such as quotes (<code>'</code>) or asterisks (<code>*</code>). If the log message that you want to match contains special characters, consider entering a substring of the log message that does not contain special characters. For example, instead of entering, <code>User 'admin' deleted report 'Report_1'</code> , you might enter <code>admin</code> .
Threshold	Set the threshold or log message level frequency that the FortiAnalyzer unit monitors for before sending an alert message. For example, set the FortiAnalyzer unit to send an alert only after it receives five emergency messages in an hour.
Destination(s)	Select where the FortiAnalyzer unit sends the alert message.
Send alert to	Select an email address, SNMP trap or Syslog server from the list. You must configure the SNMP traps or Syslog server, before you can select them from the list. For the FortiAnalyzer unit to send an email message, you must configure a DNS server and mail server account. For information, see "Configuring alerts by email server" on page 135 . For information on configuring SNMP traps, see "Configuring SNMP traps and alerts" on page 136 . For information on configuring Syslog servers, see "Configuring alerts by Syslog server" on page 140 .

From Email Address	When configuring the FortiAnalyzer unit to send an email alert message, enter the sender's email address.
To Email Address	When configuring the FortiAnalyzer unit to send an email alert message, enter the recipients' email address.
Add	Select Add to add the destination for the alert message. Add as many recipients as required.
Delete	Select a recipient from the Destination list and select Delete to remove a recipient.
Include Alert Severity	Select the alert severity value to include in the outgoing alert message information.

- 4 Select OK.

Output

When the FortiAnalyzer unit receives a log messages meeting the alert event conditions, it sends an alert message as an email, syslog message or SNMP Trap, informing an administrator of the issue and where it is occurring.

You can configure the methods FortiAnalyzer units use to send alert messages. The FortiAnalyzer unit can send an alert message to an email address via SMTP, a Syslog server or as an SNMP Trap.

Configuring alerts by email server

You must first configure an SMTP server to configure the FortiAnalyzer unit to send email alert messages,




If the mail server is defined by a domain name, the FortiAnalyzer unit will query the DNS server to resolve the IP address of that domain name. In this case, you must also define a DNS server. See ["DNS" on page 46](#) to configure a DNS server.

If sending an email by SMTP fails, the FortiAnalyzer unit will re-attempt to send the message every ten seconds, and never stop, until it succeeds in sending the message or the administrator reboots the FortiAnalyzer unit.



Note: Mail servers that you have defined for the FortiAnalyzer unit to be able to send alerts can also be selected when configuring report profiles and vulnerability scan jobs to email report output. For more information, see ["Configuring vulnerability scan jobs" on page 162](#) and ["Configuring reports" on page 113](#).

Figure 2: Mail server list

Mail Server Settings			
Create New			
SMTP Server	E-Mail Account	Password	Action
mail.company.com	admin@company.com	*****	  

Delete
 Edit
 Test

To add a mail server for alerts

- 1 Go to **Alert > Output > Mail Server**.
- 2 Select Create New.
- 3 Configure the following options:

SMTP Server	The name/address of the SMTP email server.
Enable Authentication	Select the Authentication Enable check box to enable SMTP authentication. When set, you must enter an email user name and password for the FortiAnalyzer to send an email with the account.
Email Account	Enter the user name for logging on to the SMTP server to send alert mails. You only need to do this if you have enabled the SMTP authentication. The account name must be in the form of an email address, such as <code>user@example.com</code> .
Password	Enter the password for logging on to the SMTP server to send alert email. You only need to do this if you selected SMTP authentication.

- 4 Select Apply.

Testing the mail server configuration

You can send a test email message to verify that alerts can be sent.

To verify mail server connectivity

- 1 Go to **Alert > Output > Mail Server**.
- 2 In the row corresponding the mail server that you want to verify, select Test.
- 3 Enter an email address in Send test email to.

To verify complete connectivity from the FortiAnalyzer unit to the administrator's inbox, this should be the administrator's email address.

- 4 Select Test.

A message appears, indicating the success or failure of sending email to the SMTP server. If the message was successfully sent, verify that it reached the email address.

Configuring SNMP traps and alerts

You can configure the SNMP server where the FortiAnalyzer unit sends SNMP traps when an alert event occurs, and which SNMP servers are permitted to access FortiAnalyzer SNMP system traps. You must add at least one SNMP server before you can select it as an alert destination.

For a list of supported MIBs and traps, see [“FortiAnalyzer SNMP support” on page 138](#).

To view configured SNMP servers, go to **Alert > Output > SNMP Access List**.

Figure 3: SNMP Access List

SNMP Access List

SNMP Agent Enable

Description

Location

Contact

	Trap Type	Trigger	Threshold	Sample Period(s)	Sample Frequency(s)
1	cpu	50 %	10	300	20
2	memory	23 %	5	60	60
3	disk	100 %	1	600	30

Apply

Communities:

#	Community Name	Enable	
1	example_community	<input checked="" type="checkbox"/>	<input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Test"/>

SNMP Agent	Select to enable the SNMP agent.
Description	Enter a descriptive name for this FortiAnalyzer unit.
Location	Enter the physical location of the FortiAnalyzer unit, such as a city or floor number.
Contact	Enter a contact, such as an administrator's name.
Trap Type	The type of available SNMP trap.
Trigger	Enter a number (percent) that will trigger a trap. The number can be between 1 to 100.
Threshold	Enter a number for the threshold. The number can be between 1 and 100.
Sample Period(s)	Enter a time period, in seconds. The number can be between 1 and 28800. The default number is 600 seconds, which is 10 minutes. During the configured time period, the SNMP agent evaluates the trap type, for example, CPU, at every same frequency. For example, during 600 seconds (10 minutes), the SNMP agent evaluates Memory every 60 seconds (1 minute).
Sample Frequency(s)	Enter a number for the frequency of triggers. The number can be between 1 and 100.
Apply	Select to save the configured settings. Selecting Apply will not save the SNMP communities because they are automatically saved after being configured.
Create New	Select to add a new SNMP server. This option appears only if there is no configured SNMP server. You can add more SNMP servers using the CLI. For more information, see the FortiAnalyzer CLI Reference .
#	The sequential order of the communities.
Community Name	The community name of the SNMP server.

Enable	Select to disable the SNMP community.
Action	Select Delete to remove the SNMP server configuration. Select Edit to change the SNMP server configuration. Select Test to verify the SNMP server configuration by sending a test SNMP trap. This option does not appear if the IP or FQDN is 0.0.0.0.

Adding an SNMP server

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

To add an SNMP community

- 1 Go to **Alert > Output > SNMP Access List**.
- 2 Select Create New.
- 3 Enter a name in the Community Name field.
- 4 Select Add and then enter the IP address of the host.
- 5 If you need to enter multiple hosts, repeat step 4 until all hosts are included.
- 6 If you need to disable an SNMP event in the SNMP Event list, select the check box beside the SNMP event to unselect the check box.
- 7 Select OK.

FortiAnalyzer SNMP support

You can configure the FortiAnalyzer unit to respond to traps and send alert messages to SNMP managers that you have added to SNMP communities. If the standard MIBs used by the FortiAnalyzer SNMP agent are already compiled into your SNMP manager, you do not have to recompile them.

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

For your SNMP manager to be able to communicate with the FortiAnalyzer unit, you must first compile the Fortinet proprietary MIBs and supported standard MIBs into your SNMP manager's MIB database. You can obtain the Fortinet MIB files from Fortinet Technical Support.

Your SNMP manager might already have a database of compiled standard and private MIBs. In that case, add the Fortinet proprietary MIB to this database.

The Fortinet MIB contains support for all Fortinet devices, and includes some generic SNMP traps; information responses and traps that FortiAnalyzer units send are a subset of the total number supported by the Fortinet proprietary MIB.

fnTrapFlgEventCount is associated with alerts, which arise from log messages received by the FortiAnalyzer unit from devices in the device list. All other traps sent by FortiAnalyzer units arise from events on the FortiAnalyzer unit itself.

SNMP support provided by the Fortinet MIB is listed as follows.

Fortinet MIB System Traps

- fnTrapCpuHigh
- fnTrapMemLow
- fnTrapIpChange

Fortinet MIB Logging Traps

- fnTrapLogFull

Fortinet MIB VPN Traps

- fnTrapVpnTunUp
- fnTrapVpnTunDown
- fnTrapFlgEventCount

Fortinet MIB System fields

- fnSysModel
- fnSysSerial
- fnSysVersion
- fnSysCpuUsage
- fnSysMemUsage
- fnSysSesCount
- fnSysDiskCapacity
- fnSysDiskUsage
- fnSysMemCapacity

Fortinet MIB Administrator Accounts

- fnAdminNumber
- fnAdminIndex
- fnAdminName
- fnAdminAddr

Fortinet MIB Options

- fnOptIdleTimeout
- fnOptLanguage

Fortinet MIB Active IP Sessions

- fnIpSessIndex
- fnIpSessProto
- fnIpSessFromAddr
- fnIpSessFromPort
- fnIpSessToAddr
- fnIpSessToPort
- fnIpSessExp
- fnIpSessVdom

RFC-1213 (MIB II)

- mib-2.system
- mib-2.interface
- mib-2.at
- mib-2.ip
- mib-2.icmp
- mib-2.tcp
- mib-2.udp
- mib-2.ifMIB

RFC-2665 (Ethernet-like MIB)




- .dot3StatsTable
- .dot3CollTable
- .dot3ControlTable
- .dot3PauseTable

Configuring alerts by Syslog server

You can configure Syslog servers where the FortiAnalyzer unit can send alerts. You must add the syslog server before you can select it as a way for the FortiAnalyzer unit to communicate an alert.

To view the SNMP servers, go to **Alert > Output > Syslog Server**.

Figure 4: Syslog server list

#	Name	IP or FQDN : Port	Action
1	syslog1	10.10.10.20:514	  

Create New	Select to add a new Syslog server.
Name	The name given to the Syslog server.
IP or FQDN: Port	The IP address or fully qualified domain name for the SNMP server, and port number.
Action	Select Delete to remove the Syslog server configuration. Select Edit to change the Syslog server configuration. Select Test to verify the Syslog server configuration.

Adding a Syslog server

You can add a Syslog server to send alerts by the Syslog protocol.

To add a new Syslog server

- 1 Go to **Alert > Output > Syslog Server**.
- 2 Select Create New.

- 3 Configure the following options, and select OK.
 - Name** Enter a name for the SNMP server.
 - IP address (or FQDN)** Enter the IP address or fully qualified domain name for the SNMP server.
 - Port** Enter the Syslog server port number. The default Syslog port is 514.

Network Analyzer

Network Analyzer can be used as an enhanced local network traffic sniffer to diagnose areas of the network where firewall policies may require adjustment, or where traffic anomalies occur.

Network Analyzer logs all traffic seen by the interface for which it is enabled. If that network interface is connected to the span port of a switch, observed traffic will include all traffic sent through the switch by other hosts. You can then locate traffic which should be blocked, or which contains other anomalies.

All captured traffic information is saved to the FortiAnalyzer hard disk. You can then display this traffic information directly, search it, or generate reports from it.

This section describes how to enable and view traffic captured by the Network Analyzer. It also describes Network Analyzer log storage configuration options.

Network Analyzer is not visible in **Tools > Network Analyzer** until enabled in the CLI. To enable Network Analyzer, access the CLI and enter the commands:

```
config log settings
    set enable_analyzer yes
end
```

If you are currently logged in to the web-based manager when enabling or disabling Network Analyzer, you must log out and then log in again for the menu changes to take effect.

This section includes the following topics:

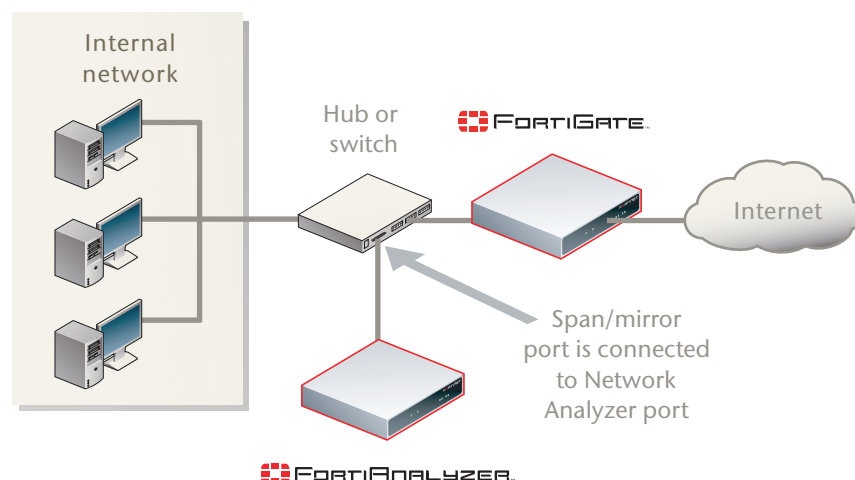
- [Connecting the FortiAnalyzer unit to analyze network traffic](#)
- [Viewing Network Analyzer log messages](#)
- [Browsing Network Analyzer log files](#)
- [Customizing the Network Analyzer log view](#)
- [Searching the Network Analyzer logs](#)
- [Rolling and uploading Network Analyzer logs](#)



Note: Network Analyzer available all FortiAnalyzer units except the FortiAnalyzer-100.

Connecting the FortiAnalyzer unit to analyze network traffic

You usually first connect the FortiAnalyzer unit to the span (or mirroring) port of an Ethernet switch to sniff traffic with the FortiAnalyzer unit. Both the management and sniffing ports can be connected to the same switch.

Figure 1: Example network topology for Network Analyzer use**To connect the FortiAnalyzer unit for use with Network Analyzer**

- 1 Connect an Ethernet cable to a port on the FortiAnalyzer unit other than the port used to collect device logs.

For example, if you receive logs and quarantined files on port 1, you might use Network Analyzer on port 2. Using a separate port for sniffing prevents log and quarantine traffic from cluttering Network Analyzer messages, and enables you to analyze networks without tampering with network settings related to normal logging and quarantine activity.

- 2 Connect the other end of the Ethernet cable to the span or mirroring port of an Ethernet switch.

If connected to the span or mirror port of a switch, Network Analyzer will be able to observe all traffic passing through the switch.

- 3 In the CLI, enable Network Analyzer on the port where you attached the Ethernet cable by entering the commands:

```
config log settings
    set enable_analyzer yes
end
```

If you are currently logged in to the web-based manager when enabling or disabling Network Analyzer, you must log out and then log in again for the menu changes to take effect.

- 4 In the web-based manager, go to **System > Network > Interface**.
- 5 If the interface you will use with Network Analyzer is currently down, select Bring Up to enable it.
- 6 Select Modify for the interface you will use with Network Analyzer.
- 7 Enter the IP/Netmask.
- 8 Select OK.

You can now configure Network Analyzer settings in **Tools > Network Analyzer > Config**.

Viewing Network Analyzer log messages

After attaching a FortiAnalyzer unit interface to the network and enabled the Network Analyzer for that interface, traffic information displays.

The Network Analyzer's log viewers display logs of traffic seen by the network interface you have configured for use with Network Analyzer, focusing on specific time frames.

The Network Analyzer has two types of log viewing options:

- Real-time displays the Network Analyzer log messages of traffic most recently observed by the network interface for which Network Analyzer is enabled. The display refreshes every few seconds, and contains only the most current activity.
- Historical displays all Network Analyzer log messages whose time stamps are within your specified time frame.

Viewing current Network Analyzer log messages

The Real-time tab in **Tools > Network Analyzer** updates continually, displaying the most recent traffic observed by the Network Analyzer.

To view the most recent traffic, go to **Tools > Network Analyzer > Real-time**.

Figure 2: Viewing current Network Analyzer logs

Column Settings

Log Time	Source	Destination	Protocol	Message
2007-04-30 10:45:10	172.20.120.139	172.20.120.46	tcp	443 -> 443 [ACK] Ack=2397849706
2007-04-30 10:45:10	172.20.120.46	172.20.120.139	tcp	1078 -> 1078 [ACK PSH] Seq=2397848950 Ack=3876537713
2007-04-30 10:45:10	172.20.120.139	172.20.120.46	tcp	443 -> 443 [ACK] Ack=2397847737
2007-04-30 10:45:10	172.20.120.46	172.20.120.139	tcp	1078 -> 1078 [ACK PSH] Seq=2397847737 Ack=3876537713
2007-04-30 10:45:10	172.20.120.46	172.20.120.139	tcp	1078 -> 1078 [ACK] Seq=2397846277 Ack=3876537713
2007-04-30 10:45:10	172.20.120.46	172.20.120.139	tcp	1078 -> 1078 [ACK] Seq=2397844817 Ack=3876537713
2007-04-30 10:45:10	1.1.1.1	255.255.255.255	arp	arp who-has 1.1.1.3 tell 1.1.1.1
2007-04-30 10:45:09	1.1.1.1	255.255.255.255	arp	arp who-has 1.1.1.3 tell 1.1.1.1
2007-04-30 10:45:09	n/a	n/a	fdp	FDP HELLO from device FortiAnalyzer
2007-04-30 10:45:08	172.20.120.132	172.20.120.139	udp	UDP length=503
2007-04-30 10:45:08	1.1.1.1	255.255.255.255	arp	arp who-has 1.1.1.3 tell 1.1.1.1
2007-04-30 10:45:06	172.20.120.139	172.20.120.131	tcp	514 -> 514 [ACK] Ack=2475302732

Stop	Select to stop the traffic sniffing. When selected, Stop changes to Start. Select Start to continue the real-time traffic viewing.
Column Settings	Select to change the columns to view and the order they appear on the page. For more information, see "Displaying and arranging log columns" on page 148.
Formatted Raw	Select a view of the Network Analyzer log file. Selecting Formatted (the default) displays the Network Analyzer log files in columnar format. Selecting Raw, displays the Network Analyzer log information as it actually appears in the log file.
Resolve Host Name	Select to display host names by a recognizable name rather than IP addresses. For more information about on configuring IP address host names see "Configuring IP aliases" on page 61.
Resolve Service	Select to display the network service names rather than the port numbers, such as HTTP rather than port 80.
Log Time	The date and time the traffic was transmitted.
Source	The IP address of the sender of the traffic.
Destination	The IP address of the recipient of the traffic.
Destination Port	The port a UDP or TCP packet was being sent to.

Protocol	The protocol used when sending the traffic.
Message	Information payload of the traffic sent through the switch.

Viewing historical Network Analyzer log messages

The Historical tab in **Tools > Network Analyzer** displays Network Analyzer logs for a specific time range. When viewing log messages, you can filter the information to find specific traffic information.

To view a historical Network Analyzer log, go to **Tools > Network Analyzer > Historical** and then select the log you want to view.

Figure 3: Viewing historical Network Analyzer logs

#	Last Activity	Source	Destination	Protocol	Message
1	2007-03-27 10:20:37	172.20.120.46	172.20.120.139	tcp	3903 -> 3903 [ACK PSH] Seq=1706099061 Ack=1065272943
2	2007-03-27 10:20:37	172.20.120.139	172.20.120.46	tcp	443 -> 443 [ACK] Ack=1706098232
3	2007-03-27 10:20:37	172.20.120.46	172.20.120.139	tcp	3903 -> 3903 [ACK PSH] Seq=1706098232 Ack=1065272943
4	2007-03-27 10:20:37	172.20.120.46	172.20.120.139	tcp	3903 -> 3903 [ACK] Seq=1706096772 Ack=1065272943
5	2007-03-27 10:20:37	172.20.120.46	172.20.120.139	tcp	3903 -> 3903 [ACK] Seq=1706095312 Ack=1065272943
6	2007-03-27 10:20:37	1.1.1.1	255.255.255.255	arp	arp who-has 1.1.1.1 tell 1.1.1.1
7	2007-03-27 10:20:36	172.20.120.139	172.20.120.132	tcp	514 -> 514 [ACK] Ack=707462431
8	2007-03-27 10:20:36	172.20.120.132	172.20.120.139	tcp	2624 -> 2624 [ACK PSH] Seq=707462407 Ack=2166361543
9	2007-03-27 10:20:36	172.20.120.139	172.20.120.132	tcp	514 -> 514 [ACK PSH] Seq=2166361515 Ack=707462407

Type	The type of log you are viewing and the device where it originated.
Change	Select to change the log, time frame or a different device.
Formatted Raw	Select a view of the log file. Selecting Formatted (the default) displays the log files in columnar format. Selecting Raw, displays the log information as it actually appears in the log file.
Resolve Host Name	Select to display host names by a recognizable name rather than IP addresses. For more information about on configuring IP address host names see "Configuring IP aliases" on page 61 .
Resolve Service	Select to display the network service names rather than the port numbers, such as HTTP rather than port 80.
View n per page	Select the number of rows of log entries to display per page.
Page n of n	Enter a page number, then press Enter to go to the page.
Column Settings	Select to change the columns to view and the order they appear on the page. For more information, see "Displaying and arranging log columns" on page 148 .
Search	Enter a keyword to perform a simple search on the log information available. Select Go to begin the search. The number of matches appears above the Search field.
Printable Version	Select to download an HTML file containing all log messages that match the current filters. The HTML file is formatted to be printable. Time required to generate and download large reports varies by the total amount of log messages, the complexity of any search criteria, the specificity of your column filters, and the speed of your network connection.
Download Current View	Select to download only those log messages which are currently visible, according to enabled filters. This button only appears when the current view is filtered.
Log Time	The date and time the traffic was transmitted.
Source	The IP address of the sender of the traffic.
Destination	The IP address of the recipient of the traffic.

Destination Port	The destination port of the traffic.
Protocol	The protocol used when sending the traffic.
Message	Information payload on the traffic sent through the switch.

Browsing Network Analyzer log files

The Browse tab in **Tools > Network Analyzer** enables you to see all stored Network Analyzer log files, view the Network Analyzer logs, download log files to your hard disk or delete unneeded files.

When a log file reaches its maximum size, the FortiAnalyzer unit saves the log files with an incremental number, and starts a new log file with the same name. The current Network Analyzer log is `xlog.log`. Any subsequent saved logs appear as `xlog.n.log`, where *n* is the number of rolled logs.

For more information about setting the maximum file size and log rolling options, see [“Rolling and uploading Network Analyzer logs” on page 153](#).

To view the log file list, go to **Tools > Network Analyzer > Browse**.

Figure 4: Network Analyzer log file list

Delete		Allocated Disk Space: 1000 MB Used Disk Space: 0 MB		
Log Files	Last Modified	Size (bytes)	Action	
<input type="checkbox"/> xlog.log	Wed Mar 7 10:39:32 2007	6,213		

Delete
Download
Display

Log files	A list of log files on the FortiAnalyzer unit.
Last Modified	The last time the log was updated from the device.
Size (bytes)	The size of the log file.
Action	Select Delete to remove the log file from the FortiAnalyzer hard disk. Select Download to save the log file to your local hard disk. Select Display to view the contents of the log file.

Viewing Network Analyzer log file contents

The Browse tab enables you to view all log messages within Network Analyzer log files.

If you display the log messages in Formatted view, you can display and arrange columns and/or filter log messages by column contents. For more information, see [“Customizing the Network Analyzer log view” on page 148](#).

To view a log file

- 1 Go to **Tools > Network Analyzer > Browse**.
- 2 In the row corresponding to the log file's row, in the Action column, select Display. The log file's contents appear.

Figure 5: Viewing Network Analyzer logs

Column Settings Printable Version

#	Last Activity	Source	Destination	Protocol	Destination Port	Message
1	2007-03-27 10:20:37	172.20.120.46	172.20.120.139	tcp	443	3903 -> 3903 [ACK PSH] Seq=1706099061 Ack=1065272943
2	2007-03-27 10:20:37	172.20.120.139	172.20.120.46	tcp	3903	443 -> 443 [ACK] Ack=1706098232
3	2007-03-27 10:20:37	172.20.120.46	172.20.120.139	tcp	443	3903 -> 3903 [ACK PSH] Seq=1706098232 Ack=1065272943
4	2007-03-27 10:20:37	172.20.120.46	172.20.120.139	tcp	443	3903 -> 3903 [ACK] Seq=1706096772 Ack=1065272943
5	2007-03-27 10:20:37	172.20.120.46	172.20.120.139	tcp	443	3903 -> 3903 [ACK] Seq=1706095312 Ack=1065272943
6	2007-03-27 10:20:37	1.1.1.1	255.255.255.255	arp		arp who-has 1.1.1.3 tell 1.1.1.1
7	2007-03-27 10:20:36	172.20.120.139	172.20.120.132	tcp	2624	514 -> 514 [ACK] Ack=707462431
8	2007-03-27 10:20:36	172.20.120.132	172.20.120.139	tcp	514	2624 -> 2624 [ACK PSH] Seq=707462407 Ack=2166361543
9	2007-03-27 10:20:36	172.20.120.139	172.20.120.132	tcp	2624	514 -> 514 [ACK PSH] Seq=2166361515 Ack=707462407
10	2007-03-27 10:20:36	172.20.120.139	172.20.120.132	tcp	2624	514 -> 514 [ACK] Ack=707462407

Type	The type of log you are viewing and the device where it originated.
Change	Select to view a different log file.
Formatted Raw	Select a view of the log file. Selecting Formatted (the default) displays the network traffic log files in columnar format. Selecting Raw, displays the network traffic log information as it actually appears in the log file.
Resolve Host Name	Select to display host names by a recognizable name rather than IP addresses. For more information about on configuring IP address host names, see “Configuring IP aliases” on page 61 .
Resolve Service	Select to display the network service names rather than the port numbers, such as HTTP rather than port 80.
View <i>n</i> per page	Select the number of rows of log entries to display per page.
Page <i>n</i> of <i>n</i>	Enter a page number, then select Go to go to the page.
Column Settings	Select to change the columns to view and the order they appear on the page. For more information, see “Displaying and arranging log columns” on page 148 .
Search	Enter a keyword to perform a simple search on the log information available. Select Go to begin the search. The number of matches appears above the Search field.
Printable Version	Select to download an HTML file containing all log messages that match the current filters. The HTML file is formatted to be printable. Time required to generate and download large reports varies by the total amount of log messages, the complexity of any search criteria, the specificity of your column filters, and the speed of your network connection.
Download Current View	Select to download only those log messages which are currently visible, according to enabled filters. This button only appears when the current view is filtered.
Log Time	The date and time the traffic was transmitted.
Source Port	The port number where the traffic originated.
Destination	The IP address of the recipient of the traffic.
Destination Port	The port a UDP or TCP packet was being sent to.
Protocol	The protocol used when sending the traffic.
Message	Information on the traffic sent through the switch.

Downloading a Network Analyzer log file

You can download a log file to save it as a backup or for use outside the FortiAnalyzer unit. You can choose to download either the entire file or only log messages selected by filtering.

To download a whole log file

- 1 Go to **Tools > Network Analyzer > Browse**.
- 2 In the Log Files column, locate a log file.
- 3 In the Action column, select Download.
- 4 Select any download options you want and select OK.

Convert to CSV format Downloads the log format as a comma-separated value (.csv) file instead of a standard .log file. Each log element is separated by a comma. CSV files can be viewed in spreadsheet applications.

Compress with gzip Compress the .log or .csv file with gzip compression. For example, downloading a log-formatted file with gzip compression would result in a download with the file extension .log.gz.

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

To download a partial (filtered) log file

- 1 Go to **Tools > Network Analyzer > Browse**.
- 2 In the Log Files column, locate a log file.
- 3 In the Action column, select Display.
- 4 Select a filter icon to restrict the current view to only items which match your criteria, then select OK.

Filtered columns now have a green filter icon, and Download Current View appears next to Printable Version.

- 5 Select Download Current View.
- 6 Select any download options you want and select OK.

Convert to CSV format Downloads the log format as a comma-separated value (.csv) file instead of a standard .log file. Each log element is separated by a comma. CSV files can be viewed in spreadsheet applications.

Compress with gzip Compress the .log or .csv file with gzip compression. For example, downloading a log-formatted file with gzip compression would result in a download with the file extension .log.gz.

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

Customizing the Network Analyzer log view

Log messages can be displayed in either Raw or Formatted view.

- Raw view displays log messages exactly as they appear in the log file.
- Formatted view displays log messages in a columnar format. Each log field in a log message appears in its own column, aligned with the same field in other log messages, for rapid visual comparison. When displaying log messages in Formatted view, you can customize the log view by hiding, displaying and arranging columns and/or by filtering columns, refining your view to include only those log messages and fields that you want to see.

To display logs in Raw or Formatted view

- 1 Go to a page which displays log messages, such as **Tools > Network Analyzer > Real-time**.
- 2 Select Formatted or Raw.

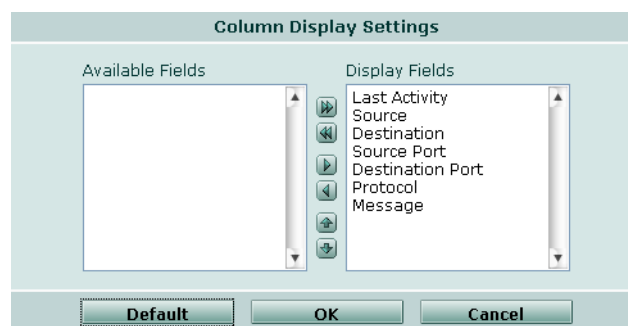
If you select Formatted, options appear that enable you to display and arrange log columns and/or filter log columns.

Displaying and arranging log columns

When viewing logs in Formatted view, you can display, hide and re-order columns to display only relevant categories of information in your preferred order.

For most columns, you can also filter data within the columns to include or exclude log messages which contain your specified text in that column. For more information, see [“Filtering logs” on page 149](#).

Figure 6: Displaying and arranging Network Analyzer log columns



To display or hide columns

- 1 Go to a page which displays log messages, such as **Tools > Network Analyzer > Real-time**.
- 2 Select Column Settings.

Lists of available and displayed columns for the log type appear.

- 3 Select which columns to hide or display.
 - In the Available Fields area, select the names of individual columns you want to display, then select the single right arrow to move them to the Display Fields area.
Alternatively, to display all columns, select the double right arrow.
 - In the Display Fields area, select the names of individual columns you want to hide, then select the single left arrow to move them to the Available Fields area.
Alternatively, to hide all columns, select the double left arrow.
 - To return all columns to their default displayed/hidden status, select Default.
- 4 Select OK.

To change the order of the columns

- 1 Go to a page which displays log messages, such as **Tools > Network Analyzer > Real-time**.
- 2 Select Column Settings.
Lists of available and displayed columns for the log type appear.
- 3 In the Display Fields area, select a column name whose order of appearance you want to change.
- 4 Select the up or down arrow to move the column in the ordered list.
Placing a column name towards the top of the Display Fields list will move the column to the left side of the Formatted log view.
- 5 Select OK.

Filtering logs

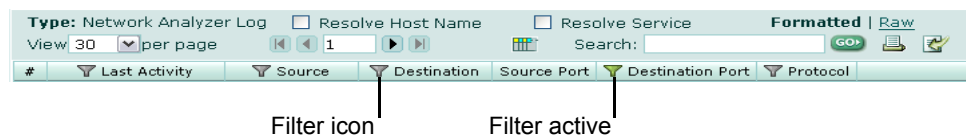
When viewing log messages in Formatted view, you can filter columns to display only those log messages that do or do not contain your specified content in that column. By default, most column headings contain a gray filter icon, which becomes green when a filter is configured and enabled.



Note: Filters do not appear in Raw view, or for unindexed log fields in Formatted view.

When viewing real-time logs, you cannot filter on the time column: by definition of the real-time aspect, only current logs are displayed.

Figure 7: Filter icons in Network Analyzer



To filter log messages by column contents

- 1 In the heading of the column that you want to filter, select the filter icon.
- 2 Select Enable.

- 3 If you want to *exclude* log messages with matching content in this column, select NOT.

If you want to *include* log messages with matching content in this column, deselect NOT.

- 4 Enter the text that matching log messages must contain.

Matching log messages will be excluded or included in your view based upon whether you have selected or deselected NOT.

- 5 Select OK.

A column's filter icon is green when the filter is currently enabled. A Download Current View icon also appears, enabling you to download only log messages which meet the current filter criteria.

To disable a filter

- 1 In the heading of the column whose filter you want to disable, select the filter icon.

A column's filter icon is green when the filter is currently enabled.

- 2 To disable the filter on this column, deselect Enable.

Alternatively, to disable the filters on all columns, select Clear All Filters. This disables the filter; it does not delete any filter text you might have configured.

- 3 Select OK.

A column's filter icon is gray when the filter is currently disabled.

Filtering tips

When filtering by source or destination IP, you can use the following in the filtering criteria:

- a single address (2.2.2.2)
- an address range using a wild card (1.2.2.*)
- an address range (1.2.2.1-1.2.2.100)

You can also use a Boolean operator (`OR`) to indicate mutually exclusive choices:

- 1.1.1.1 `OR` 2.2.2.2
- 1.1.1.1 `OR` 2.2.2.*
- 1.1.1.1 `OR` 2.2.2.1-2.2.2.10

Most column filters require that you enter the column's entire contents to successfully match and filter contents; partial entries do not match the entire contents, and so will not create the intended column filter.

For example, if the column contains a source or destination IP address (such as 192.168.2.5), to create a column filter, enter the entire IP address to be matched. If you enter only one octet of the IP address, (such as 192) the filter will not completely match any of the full IP addresses, and so the resulting filter would omit all logs, rather than including those logs whose IP address contains that octet.

Exceptions to this rule include columns that contain multiple words or long strings of text, such as messages or URLs. In those cases, you may be able to filter the column using a substring of the text contained by the column, rather than the entire text contained by the column.

Searching the Network Analyzer logs

You can search the Network Analyzer log files for matching text using two search types: Quick Search and Full Search.

You can use Quick Search to find results more quickly if your search terms are relatively simple and you only need to search indexed log fields. Indexed log fields are those that appear with a filter icon when browsing the logs in column view; unindexed log fields do not contain a filter icon for the column or do not appear in column view, but do appear in the raw log view. Quick Search keywords cannot contain:

- special characters such as single or double quotes (` ` or ` `) or question marks (?)
- wild card characters (*), or only contain a wild card as the last character of a keyword (logi*)

You can use Full Search if your search terms are more complex, and require the use of special characters or log fields not supported by Quick Search. Full Search performs an exhaustive search of all log fields, both indexed and unindexed, but is often slower than Quick Search.

Figure 8: Network Analyzer log search

Date	Select to search logs from a time frame, or select Specify and define a custom time frame by selecting the From and To date and times.
From	Enter the date and select the time of the beginning of the custom time range. This option appears only when Date is Specify.
To	Enter the date and select the time of the end of the custom time range. This option appears only when Date is Specify
Keyword(s)	Enter search terms which will be matched to yield log message search results. To specify that results must include all, any, or none of the keywords, select from Match.
Quick Search	Select to perform a Quick Search, whose Keywords cannot contain special characters and that searches only indexed fields.
Full Search	Select to perform a Full Search, whose Keywords may contain special characters, and searches all log message fields. The time of the search varies by the complexity of the search query and the amount of log messages to be searched.

More Options Select the blue arrow to hide or expand additional search options.

Other

Specify additional criteria, if any, that can be used to further restrict the search criteria.

- **Source IP:** Enter an IP address to include only log messages containing a matching source IP address. For example, entering `192.168.2.1` would cause search results to include only log messages containing `src=192.168.2.1`.
- **Destination IP:** Enter an IP address to include only log messages containing a matching destination IP address. For example, entering `192.168.2.1` would cause search results to include only log messages containing `dst=192.168.2.1`.

To search the logs

- 1 Go to **Tools > Network Analyzer > Search**.
- 2 From Date, select Any time to search log messages from all time periods, select a predefined time period, or select Specify and then define the starting and ending time of your custom time period.
- 3 In Keyword(s), enter your search criteria.
- 4 If you want to specify additional match or filter criteria, select More Options to expand that area, then configure those options.
- 5 Select Quick Search or Full Search.

Time required to retrieve search results varies by the complexity of the search query, the amount of log data being searched, and whether you select Quick Search or Full Search.

Search tips

If your search does not return the results you expect, but log messages exist that should contain matching text, examine your keywords and filter criteria using the following search characteristics and recommendations.

- Separate multiple keywords with a space (`arp who-has 1.1.1.1`).
- Keywords cannot contain unsupported special characters. Supported characters vary by selection of Quick Search or Full Search.
- Keywords must literally match log message text, with the exception of case insensitivity and wild cards; resolved names and IP aliases will not match.
- Some keywords will not match unless you include both the log field name and its value, surrounded by quotes (`"Ack=2959769124"`).
- Remove unnecessary keywords and search filters which can exclude results. For a log message to be included in the search results, *all* keywords must match; if any of your keywords does not exist in the message, the match will fail and the message will not appear in search results.
- You can use the asterisk (*) character as a wild card (`192.168.2.*`). For example, you could enter any partial term or IP address, and then enter * to match all terms that have identical beginning characters or numbers.

- You can search for IP ranges, including subnets. For example:
 - `172.168.1.1/24` or `172.168.1.1/255.255.255.0` matches all IP addresses in the subnet `172.168.1.1/255.255.255.0`
 - `172.168.1.1-140.255` matches all IP addresses from `172.168.1.1` to `172.168.140.255`
- The search returns results that match all of the search terms.
For example, consider two similar keyword entries: `172.20.120.127 tcp` and `172.20.120.127 udp`. If you enter the keywords `172.20.120.127 tcp`, UDP traffic would not be included in the search results, since although the first keyword (the IP address) matches, the second keyword, `tcp`, does not match.
- The search returns results that match all, any, or none of the search terms, according to the option you select in Match.
For example, if you enter into Keyword(s):
`172.20.120.127 tcp`
and if from Match you select All Words, log messages for UDP traffic to `172.20.120.127` do not appear in the search results, since although the first keyword (the IP address) appears in log messages, the second keyword (the protocol) does not match UDP log messages, and so the match fails for UDP log messages. If the match fails, the log message is not included in the search results.

Printing the search results

After completing a search, a Printable Version button appears, allowing you to download a printable HTML copy of the search results.

Select the Printable Version button to download the results. You can print this file, save it to your computer for later use, or email it.

Downloading the search results

The FortiAnalyzer unit enables you to download the results of a search.

After completing a search, a Download Current View button appears. Select the button to download the results.

Search results can be saved in comma-separated value (`.csv`) format or in standard log (`.log`) format.



Note: Large logs require more time to download. Download times can be improved by selecting Compress with gzip.

To download log search results

- 1 Go to **Tools > Network Analyzer > Search**.
- 2 Perform a search using either basic or advanced search.
If your search finds one or more matching log events, a Download Current View button appears next to the Printable Version button.
- 3 Select Download Current View.
Options appear for the download's file format and compression.

- 4 Select the download options that you want, then select OK.

- | | |
|------------------------------|---|
| Convert to CSV format | Downloads the log format as a comma-separated value (.csv) file instead of a standard .log file. Each log element is separated by a comma. CSV files can be viewed in spreadsheet applications. |
| Compress with gzip | Compress the .log or .csv file with gzip compression. For example, downloading a log-formatted file with gzip compression would result in a download with the file extension .log.gz. |
- 5 If prompted by your web browser, select a location to save the file, or open it without saving.

Rolling and uploading Network Analyzer logs

You can control log file size and manage log file consumption of the FortiAnalyzer disk space with log rolling and uploading.

The Network Analyzer captures a very detailed network traffic information, and its log volume can consume the FortiAnalyzer unit's hard disk space more rapidly than standard logs. Rolling and uploading logs frees hard disk space to collect further data.

As the FortiAnalyzer unit receives new log items, it performs the following tasks:

- verifies whether the log file has exceeded its file size limit
- if the file size is not exceeded, checks to see if it is time to roll the log file. You configure the time to be either a daily or weekly occurrence, and when the roll occurs

When a log file reaches its maximum size, or reaches the scheduled time, the FortiAnalyzer unit saves the log files with an incremental number, and starts a new log file with the same name. For example, the current attack log is `xlog.log`. Any subsequent saved logs appear as `xlog.n.log`, where *n* is the number of rolled logs.

If you have enabled log uploading, you can choose to automatically delete the rolled log file after uploading, thereby limiting the amount of disk space used by rolled log files.

To enable log rolling, or to disable Network Analyzer, go to **Tools > Network Analyzer > Config**.

Figure 9: Traffic Log Settings

Enable Network Analyzer on

Select the port on which Network Analyzer observes traffic. If you disable this option and log out, Network Analyzer will be hidden in the web-based manager menu. For more information about on re-enabling Network Analyzer and making it visible again, see [“Connecting the FortiAnalyzer unit to analyze network traffic” on page 141](#).

Allocated Disk Space (MB)

Enter the amount of disk space reserved for Network Analyzer logs. The dialog also displays the amount used of the allocated space.

When Allocated Disk Space is All Used

Select what the FortiAnalyzer unit does when the allocated disk space is filled up. Select to either overwrite the older log file or stop logging until you can clear some room. To avoid completely filling the hard disk space, use the log rolling and uploading options.

Reuse settings from standard logs

Select to use the same log rolling and uploading settings that you set for standard logs files configured in **Logs > Config**.

Log rolling settings

Define when the FortiAnalyzer unit should roll its Network Analyzer log files.

Log file should not exceed

Enter the maximum size of each Network Analyzer log file. When the log file reaches the specified maximum size, the FortiAnalyzer unit saves the current log file with an incremental number and starts a new active log file. For example, if the maximum size is reached, the current `xlog.log` is renamed to `xlog.n.log`, then a new `xlog.log` is created to receive new log messages.

Log file should be rolled... even if size is not exceeded

Set the time of day when the FortiAnalyzer unit renames the current log file and starts a new active log file.

- **Daily:** Roll log files daily, even if the log file has not yet reached maximum file size.
- **Weekly:** Roll log files weekly, even if the log file has not yet reached maximum file size.
- **Optional:** Roll log files only when the log file reaches the maximum file size, regardless of time interval.

Enable log uploading	Select to upload log files to a server when a log file rolls.
Server type	Select the protocol to use when uploading to the server: <ul style="list-style-type: none">• File Transfer Protocol (FTP)• Secure File Transfer Protocol (SFTP)• Secure Copy Protocol (SCP)
Server IP address	Enter the IP address of the log upload server.
Username	Enter the user name required to connect to the upload server. By default, the user name is <code>anonymous</code> ; select the field to enter a different user name.
Password	Enter the password required to connect to the upload server.
Confirm Password	Re-enter the password to verify correct entry.
Directory	Enter a location on the upload server where the log file should be saved.
Upload Files	Select when the FortiAnalyzer unit should upload files to the server. <ul style="list-style-type: none">• When rolled: Uploads logs whenever the log file is rolled, based upon Log file should be rolled.• Daily at <i>hh:mm</i>: Uploads logs at the configured time, regardless of when or what size it rolls at according to Log file should be rolled.
Upload rolled files in gzipped format	Select to compress the log files in gzipped format before uploading to the server.
Delete files after uploading	Select to remove the log file from the FortiAnalyzer hard disk once the FortiAnalyzer unit completes the upload.

Tools

The Tools menu provides vulnerability scanning as well as viewing the files that are on your FortiAnalyzer unit. These tools help administrators either when issues appear or when trying to determine if there are any vulnerabilities on targeted hosts.

The Vulnerability Scan feature scans for open TCP and/or UDP ports on your designated target hosts. If you provide Vulnerability Scan with administrative login credentials for the target hosts, Vulnerability Scan will also log in to audit installed software for vulnerabilities such as missing patches, incorrect permissions, local exploits, and buffer overflows. When the vulnerability scan job is complete, the FortiAnalyzer unit generates a report that describes the discovered security issues and their known solutions.

Vulnerability Scan includes remote vulnerability scan (RVS) modules suitable for scanning many types of hosts, including those running Microsoft Windows or Unix variants such as Linux and Apple Mac OS X, as well as a variety of applications and services/daemons. For more information about software and vulnerability checks supported by the scan modules, see [“Viewing vulnerability scan modules” on page 161](#).

File Explorer provides information about what files are on your FortiAnalyzer unit. Accessing these files helps administrators when trying to solve an issue with support's help. File Explorer does not appear for ADOM users.

This section includes the following topics:

- [Preparing for the vulnerability scan job](#)
- [Viewing vulnerability scan modules](#)
- [Configuring vulnerability scan jobs](#)
- [Viewing vulnerability scan reports](#)
- [File Explorer](#)



Note: Vulnerability Scan is available on the FortiAnalyzer-100A and B units.

Preparing for the vulnerability scan job

For best results, before running a vulnerability scan job, you will want to plan for the type of scans that you want to perform. You may also need to configure each target host and any intermediate NAT or security devices to allow the vulnerability scan to properly reach the target hosts.

For a full scan, using all vulnerability scan modules specified in the vulnerability scan job, you must configure the vulnerability scan job with administrator or root login credentials to the target host; without administrator or root login credentials, the vulnerability scan may be limited to a port scan, or may be unable to accurately complete certain probes, as modules are limited by the privileges of the account that you configure in the vulnerability scan job. For example, users

authenticating without root or administrator credentials are typically not able to view sensitive areas of the system software or configuration; scans involving those parts cannot be accurately assessed without administrator credentials. You may also be required to modify the target host's security policy to allow the connections and to ensure that the account uses administrator account privileges when authenticating remotely. Some vulnerability scan modules, such as those that test for denial of service (DoS) attack vulnerability by simulation, can result in degraded network performance during the scan. For all of these reasons, you may want to work with the owners of target hosts to schedule an appropriate time. For example, you might schedule to avoid peak traffic hours, to restrict unrelated network access, to configure a local or domain administrator account for the express purpose of the vulnerability scan, and to ensure that the target hosts will not be powered off during the vulnerability scan.

Required preparation varies by the operating system or other installed software on target host, and by the vulnerability scan modules that you want to use. For more information about preparing Windows and Unix variant operating systems for a vulnerability scan, see [“Preparing Windows target hosts” on page 158](#) and [“Preparing Unix target hosts” on page 160](#).

You may want to consider temporarily removing obstacles that prevent the vulnerability scan from reliably connecting to the intended target hosts on the required standard port numbers. If you do not remove the obstacles, the vulnerability scan may contain false negatives or may be unable to complete a full scan. However, some vulnerability scan obstacles are typical network security or other infrastructure, so removing or disabling them can involve some risk. In this case, you will want to consider whether or not you require a full scan, and how to negate or mitigate any risk during the scan. Examples of vulnerability scan obstacles include:

- intrusion prevention systems (IPS)
- dynamic NAT
- port forwarding
- firewalls, including FortiGate units and FortiClient installations

Consider also the perspective from which you are performing the vulnerability scan, and your network's routing or other configuration to ensure that you do not scan target hosts outside your intended network space. For example, if you want to assess vulnerability from the perspective of the external network, but do not wish to impact the private network of a business partner whose network is connected to yours, you may want to connect the FortiAnalyzer unit to the external network while running the vulnerability scan job, and to carefully restrict the IP addresses and routing of traffic to target host IP addresses.

Preparing Windows target hosts

Vulnerability scan modules targeting Microsoft Windows hosts require the ability to log in to the target host using the NetBIOS protocol. If NetBIOS is not already enabled on target hosts running Windows, you must enable it for the duration of the vulnerability scan.

Some vulnerability scan modules, such as those that test file permissions or check installed patch and software versions, require full access to the target host. Vulnerability scan modules for Microsoft Windows hosts specifically require an administrator account with access to not only the file system but also the registry. You must configure the vulnerability scan job with the user name and password of an administrator account to perform a full scan using all modules,.

You can provide the vulnerability scan with an administrator account by creating a new local or domain administrator account, rather than providing an existing administrator account. However, many Windows hosts are configured so that accounts authenticating over the network inherit guest privileges, rather than the administrator privileges they would normally use when logging in locally. Guest privileges are not sufficient for all vulnerability scan modules. Change the network access security policy for accounts to Classic: local users authenticate as themselves to ensure that all modules have the privileges that they require to function correctly when authenticating remotely, for the duration of the vulnerability scan.



Caution: Configuration changes necessary for a full vulnerability scan can temporarily introduce additional risks. If possible, use a firewall or other method of mitigation, such as FortiClient, to limit which hosts can access the target host during the vulnerability scan, allowing only connections from the FortiAnalyzer, and undo any vulnerability scan configuration changes after the scan.

To configure the security policy for local accounts authenticating remotely (Windows XP)

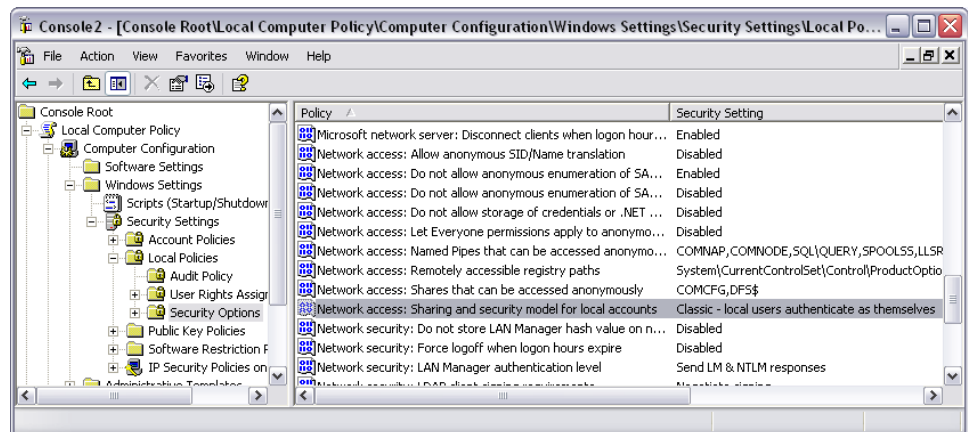
The following procedure describes how to modify the local security policy of a Windows XP target host for which you have configured a local administrator account. This procedure may vary for other versions of Windows, or for target hosts whose security policy and user accounts are administered at the domain level rather than locally to each host.

- 1 Go to **Start > Run**, enter `mmc`, and then select OK to start the Microsoft Management Console.
- 2 If a security policy console file already exists, select **File > Open** to open the existing console file.
If no security policy console file exists, select **File > New** to create a new console file.



Caution: Use care when creating a domain or local security policy, and verify that there is no pre-existing security policy. If you are unsure whether or not there is already an existing security policy in effect, consult the owner of the system. Creating a new console may overwrite any existing policy, including applying default values to settings that you have not modified specifically for the remote vulnerability scan.

- 3 If the console root does not contain Local Computer Policy (a Group Policy Object Editor snap-in that is stored on the local computer), you must add that snap-in. For instructions, see the help for the Microsoft Management Console.

Figure 1: Configuring the security model for local accounts authenticating remotely

- 4 Select Local Computer Policy.
- 5 Select Computer Configuration.
- 6 Select Windows Settings.
- 7 Select Security Settings.
- 8 Select Local Policies.
- 9 Select Security Options.
- 10 Double-click Network access: Sharing and security model for local accounts. (Alternatively, right-click and select Properties.)
- 11 Select Class - local users authenticate as themselves.
- 12 Select OK.

The setting takes effect immediately, and must remain in effect for the duration of the vulnerability scan for it to function correctly. However, if the target host is connected to a domain and this policy conflicts with the domain or other security model with higher precedence, the policy may be overridden during the next Group Policy object refresh. For more information about on policy precedence and policy object refreshes, see the help for the Microsoft Management Console.

- 13 After the vulnerability scan job completes, revert the setting configured in step 11.

To enable NetBIOS

- 1 Go to **Start > Control Panel**.
- 2 Double-click Network Connection.
- 3 Right-click Local Area Connection, and select Properties.

If this host has most than one connection, configure the connection through which the vulnerability scan will connect.

- 4 In the area labeled, "This connection uses the following items:", select Internet Protocol (TCP/IP).
- 5 Select Properties.
- 6 Select Advanced.
- 7 Select the WINS tab.
- 8 In the NetBIOS setting area, select Enable NetBIOS over TCP/IP.

- 9 Select OK.
- 10 Select OK.
- 11 Select Close.
- 12 After the vulnerability scan job completes, revert the NetBIOS settings configured in this procedure.

Preparing Unix target hosts

Vulnerability scan modules targeting Unix variant hosts, including Linux and Apple Mac OS X, require the ability to log in to the target host using the secure shell (SSH) protocol. If SSH is not already installed and/or enabled on target hosts running Unix variants, you must install and/or enable it for the duration of the vulnerability scan.

Some vulnerability scan modules, such as those that test file permissions or check installed patch and software versions, require full access to the target host. You must configure the vulnerability scan job with the user name and password of the root account on the target host to perform a full scan using all modules. Alternatively, you can provide the user name and password of an account assigned to the root user group — that is, a user account whose group ID (`gid`) is zero (0).

The root account on some Unix variants, including Apple Mac OS X, is disabled by default. In this case, you must first enable the root account, or create a new user account and assign it to the same user group as the root account. Steps to enable the root account vary by Unix variant.

If you do not enable and provide the root account, or an account with equivalent permissions, the vulnerability scan report may contain false negatives, false positives, or other inaccuracies. For example, non-root accounts are restricted to fewer commands, may be jailed, and cannot fully check the system configuration. Without root access, the vulnerability scan will be able to check only a part of the known security concerns for the host. For example, a non-root account could view the `/etc/passwd` file which contains user names, and specifies functions available to the user, but not the `/root/.bashrc` file which specifies system-wide functions.



Caution: Configuration changes necessary for a full vulnerability scan can temporarily introduce additional risks. If possible, use a firewall or other method of mitigation, such as FortiClient, to limit which hosts can access the target host during the vulnerability scan, allowing only connections from the FortiAnalyzer, and undo any vulnerability scan configuration changes after the scan.

Viewing vulnerability scan modules

The Modules page displays available remote vulnerability scan (RVS) modules. Each module tests for the presence of a specific security vulnerability on the operating system, services/daemons, applications, or other software installed on the target host, as described in the module's details.

When configuring a full vulnerability scan, you can restrict the scan job to use only those modules for vulnerabilities that meet or exceed your specified severity threshold. For more information, see [“Configuring vulnerability scan jobs” on page 162](#).

Supported operating systems and other details are located in each module’s details. Depending on the operating system and other installed software on your target hosts for which you want to assess vulnerabilities, and the severity threshold of modules that you select for the vulnerability scan, your preparation may differ. For more information, see [“Preparing for the vulnerability scan job” on page 157](#).

Update RVS modules before you begin the vulnerability scan job to ensure that your vulnerability scan job tests for the presence of the most currently known vulnerabilities. Modules and engine updates are provided by the RVS subscription service, through the Fortinet Distribution Network (FDN). For more information about RVS updates, see [“FortiGuard Center” on page 71](#).

To view available vulnerability scan modules, go to **Tools > Vulnerability Scan > Module**. To view the modules associated with that severity threshold, you can filter the display of the Modules page.

Figure 2: Vulnerability Scan modules

Name	Severity	Descriptions	Details
Applications			
Remote Access			
Kerio.MailServer.gain.shell	High	Checks for Kerio MailServer	Details
IMSP.Buf.Overflow	High	cyrus-impd abook_dbname buffer overflow	Details
Samba.buf.overflow	High	checks samba version	Details
Telnet.Serv.Get.Access	High	Remote system compromise through insecure telnet proxy	Details
apcpsd.chk.buf.overflow	High	Checks the version of apcpsd	Details
l2tpd.gain.root	High	Determines the version of the remote l2tpd	Details
INN.Control.Msg.Overflow	High	Checks INN version	Details
Samba.server.gain.root	High	checks samba version	Details
Apache.mod_mylo.module.buf.of	High	Checks for version of mod_mylo	Details
Squid.Remote.NTLM.auth.buf.of	High	Squid Remote NTLM auth buffer overflow	Details
IMAP.Server.Flaw	High	Determines the version number of the remote IMAP server	Details
Informix.traversal	High	Informix traversal	Details
IIS.Frontpage.gain.shell	High	IIS Frontpage MS03-051	Details
Simple.PHP.Blog.Installed	High	Simple PHP Blog dir traversal	Details
3com.SuperStack.user_settings	High	Obtains the remote user_settings.cfg	Details
Server.Read.ArbitraryFiles	High	\\.\\.\\.file.txt	Details
HP.JetAdmin.gain.root	High	HP JetAdmin 6.5 or less vulnerability	Details
HPJetAdmin.directory.traversal	High	HP JetAdmin directory traversal attack	Details
Web Server			
Web App			
Misc			
File Transfer			
Database			
RPC			
Snmp			
Email			
Operating System			
Web Client			
Backdoor			
P2P			
Tools			
Worm			
DOS			
IM			
Name Server			

View modules with severity

Select the subset and severity of modules that you want to view, then select Go.

Go

Select to view modules of your selected severity threshold.

Name	The name of the module group or module. Select the blue arrow to expand a module group. Module groups are organized by the type of vulnerability or the software which is susceptible.
Severity	The severity level of the vulnerability tested by the module.
Description	A brief description of the test performed by the module.
Details	Select to view additional information on the vulnerability tested by the module, including impact of potential exploits, known solutions, and affected software.

To filter the module view by vulnerability threshold

- 1 Go to **Tools > Vulnerability Scan > Module**.
- 2 From View modules with severity, select the subset:
 - ==: equal to
 - >=: greater than or equal to
 - <=: less that or equal to

then select the severity level of modules that you want to view. For example, you might view modules that test for vulnerabilities with a severity `>= Medium`.

- 3 Select Go.

To view vulnerability details

- 1 Go to **Tools > Vulnerability Scan > Module**.
- 2 Select the blue arrows to expand the module group.
- 3 In the row corresponding to the module, select Details.

Details of the vulnerability tested by that module appear, such as impact of potential exploits, known solutions, and affected software.

Configuring vulnerability scan jobs

Creating a vulnerability scan job performs an immediate or scheduled vulnerability scan, and generates a report of scan results.

Before running a vulnerability scan job, you may need to prepare the network and target hosts for the vulnerability scan job. You may also want to update the RVS modules and engine to ensure that the report tests for the latest known security issues. For more information about preparing for a vulnerability scan job, see [“Preparing for the vulnerability scan job” on page 157](#). For more information about RVS updates, see [“FortiGuard Center” on page 71](#).

When configuring a vulnerability scan job, you can configure a quick scan, or you can configure a custom scan. Quick scans perform port scan on certain standard TCP and UDP ports for services with known vulnerabilities. For a list of port numbers probed by a quick scan, see the Fortinet Knowledge Center article [Remote Vulnerability Scan Quick Scan ports](#).

Configuring a custom scan allows you to provide the user name and password of an administrator or root account for modules that require full access, and to specify the severity threshold of vulnerabilities for which you want to scan, giving you greater control over which modules will be used to probe the target host. By providing login credentials and a low severity threshold, you can perform a full scan, using all available modules. For more information about viewing the modules associated with a given severity, see [“Viewing vulnerability scan modules” on page 161](#).

Even if a user name and password are not specified in the vulnerability scan job, vulnerability scans always attempts to log in to Windows target hosts with the following combinations:

- Administrator without a password
- Administrator with a password of “Administrator”
- Guest with a random password to test for the presence of Guest accounts
- No user name or password to test Null sessions

This allows you to scan for vulnerabilities associated with weak or default user account security policies without providing an administrator login or performing many of the other Windows-related vulnerability scan modules.

To view current or scheduled vulnerability scan jobs, go to **Tools > Vulnerability Scan > Job**.

Figure 3: Vulnerability Scan jobs

Create New		Delete		
<input type="checkbox"/>	Job Name	Target	Status	Action
<input type="checkbox"/>	tvulnscan1	172.168.1.2	0%	
<input type="checkbox"/>	tvulnscan2	172.168.1.3	Waiting to start ...	
<input type="checkbox"/>	tvulnscan3	172.168.1.4	None Schedule	

Labels for Action icons: Delete, Edit, Stop job, Run now

Create New	Select to add a vulnerability job to the queue.
Delete	Select the check box of each vulnerability scan job that you want to delete, then select Delete.
Job Name	The name of the vulnerability scan job.
Target	The IP address(es) of the host(s) that the FortiAnalyzer unit will scan.
Status	The activity status of the vulnerability scan job in the queue. This can include the current activity, such as running or preparing to start, or it can be the date and time that the vulnerability scan job will run in the future. When completed, vulnerability scan job results appear in the list of vulnerability scan reports. For more information, see “Viewing vulnerability scan reports” on page 166 .
Action	Select the Delete icon to remove the vulnerability scan job from the list. Select Edit to modify the vulnerability scan job. You cannot modify a vulnerability scan job if it is currently running. Select Run now to initiate the vulnerability scan job. Select Stop job to cancel a vulnerability scan job if it is currently running.

To configure a vulnerability scan job

- 1 Go to **Tools > Vulnerability Scan > Job**.
- 2 Select Create New.
- 3 Complete the following:

Job Name Enter a name for the vulnerability scan job. This name will also be used for the report generated from scan results.

Scan Targets Enter the IP addresses, or range of addresses, of the device or hosts you want the FortiAnalyzer to scan, then select Add. The target host(s) appears in the Scan Targets area.
To remove a target host, select the target host item, then select Remove.

- 4 Select the blue arrow to expand Scan Option.
- 5 Complete the following:

Remote Authentication Enable to configure the FortiAnalyzer unit to log in to the target hosts, then also configure User Name and Password. This User Name and Password will be used to log in to each of the target hosts.

Some vulnerability scan modules require full access, such as those that probe for correct file permissions and application vulnerabilities. If you do not provide administrator or root login, some vulnerability scan modules may not be able to obtain complete or accurate results. For more information, see [“Viewing vulnerability scan modules” on page 161](#).

User Name Enter the user name for the target host(s). This option is only available after selecting Remote Authentication.

Password Enter the password for the target host(s). This option is only available after selecting Remote Authentication.

Quick Scan Select to perform a quick port scan only.
This option checks a list of common ports, and does not scan every possible port. For a list of ports scanned by this option, see the Knowledge Center article [Remote Vulnerability Scan Quick Scan ports](#).

Custom Scan Select to perform a port scan of ports that you specify in TCP Ports Range and UDP Ports Range, and also perform the vulnerability scan modules that you have selected in Modules Severity.

Modules Severity Select the severity level of vulnerability scan modules to use with the vulnerability scan job. For greatest detail, select >=Information. This option is available only after selecting Custom Scan.

For more information about on what the FortiAnalyzer unit scans, at a given severity level, see [“Viewing vulnerability scan modules” on page 161](#).

Test for reachability (Ping) before scanning each host (recommended) Select to ping each target host before performing tests defined in the scan modules. If the target host does not respond to the ping, the FortiAnalyzer unit will not perform further scans on the unresponsive host. This can accelerate scans of multiple target hosts when some of the target hosts are unavailable.

TCP Ports Range Enter the TCP port numbers, or port ranges, the FortiAnalyzer unit will port scan. Separate each port number or range of numbers with a comma. This option is available only after selecting Custom Scan.

- Enable UDP scan** Select to run a port scan on UDP ports. This option is available only after selecting Custom Scan.
- UDP Ports Range** Enter the UDP port numbers, or port ranges, the FortiAnalyzer unit will port scan. Separate each port number or range of numbers with a comma. This option is available only after selecting Custom Scan.

6 Select the blue arrow to expand Schedule Option.

7 From Schedule, select either Run Now or Run Later.

If you select Run Later, also select the Date or Time when the FortiAnalyzer unit will run the scan. For example, you might run the vulnerability scan at night when log traffic demands fewer of the FortiAnalyzer unit's resources, and when target hosts can be dedicated to the scan. For additional information on scan preparation requirements, see [“Preparing for the vulnerability scan job” on page 157](#).

8 Select the blue arrow to expand Output Option.

9 Complete the following:

File output If you want to save the report to the FortiAnalyzer hard disk, select one or more file formats.
Select from the following:

- HTML
- PDF
- MS Word (RTF)

See [“Viewing vulnerability scan reports” on page 166](#) to view finished reports stored on the FortiAnalyzer unit's hard disk.

Email output If you want to email the report as an email attachment, select one or more file formats.
Select from the following:

- HTML
- PDF
- MS Word (RTF)

You must also configure required email fields such as Email subject, Email Body, Email to, and Email server to complete the email output configuration.

Email subject Enter a subject for the report email. If you do not enter a subject, the subject line will be the name of the report.
This option becomes available only if at least one option in Email output is enabled.

Email Attachment Name Enter the name for the report files included in the email. If you select multiple file formats in Email output, the FortiAnalyzer unit compresses all reports into a .zip file, and this field names the .zip file.
This option becomes available only if at least one option in Email output is enabled.

Email Body Enter text to include in the body of the email message.
This option becomes available only if at least one option in Email output is enabled.

Email from Enter a sender email address for the FortiAnalyzer unit or administrator configuring the report.
This option becomes available only if at least one option in Email output is enabled.

Email server	Select which email server to use when the FortiAnalyzer unit sends reports as an email. This option becomes available only if at least one option in Email output is enabled. To define a new email server, see “Configuring alerts by email server” on page 135 .
Email to	Enter the email addresses of the recipients of the report. Add multiple recipients by pressing the Enter key after each email address. The addresses appear in Email list. This option becomes available only if at least one option in Email output is enabled.
Email list	Displays email addresses added to the recipient list through the Email to field. This option becomes available only if at least one option in Email output is enabled.

10 Select OK.

Viewing vulnerability scan reports

The Report tab in **Tools > Vulnerability Scan** displays a list of the finished vulnerability scan reports.

Vulnerability scan reports reflect the results of the vulnerability scan job, and include both summaries and detailed module test results for each target host. If the vulnerability scan job detected a vulnerability on the target host, the vulnerability scan report includes additional information about the vulnerability and potential solutions, such as patches supplied by the vendor or other mitigation techniques. Detected vulnerabilities sometimes may include false positives or false negatives if there are obstacles that prevent a thorough or accurate vulnerability scan, or if you have introduced obfuscation techniques that prevent accurate fingerprinting of the software installed on the target host, such as intentionally masking the version number or type of installed software. Vulnerability scan results will be most accurate with proper preparation before the vulnerability scan job. For more information, see [“Preparing for the vulnerability scan job” on page 157](#).

Vulnerability scan job reports will not appear in the list of vulnerability scan job reports before the vulnerability scan job is completed. See [“Configuring vulnerability scan jobs” on page 162](#) to display a list of vulnerability scan jobs that are still pending or in progress.

Figure 4: Vulnerability Scan reports

Delete					
<input type="checkbox"/>	Job Name	Start Time	End Time	Formats	Action
<input type="checkbox"/>	twlnscan3_1	2008-02-29 09:55:15	2008-02-29 09:58:11	PDF MSWord	
<input type="checkbox"/>	twlnscan2_1	2008-02-29 09:48:05	2008-02-29 09:54:17	PDF	
<input type="checkbox"/>	twlnjob1_3	2007-06-02 10:30:03	2007-06-02 10:33:05		

Delete

Delete	Select the check box of each vulnerability scan report that you want to delete, then select Delete.
Job Name	Select to view the vulnerability scan report in an HTML file format.
Start Time	The time the FortiAnalyzer unit started the vulnerability scan job.

End Time	The time the FortiAnalyzer unit completed the vulnerability scan job.
Formats	Select to view the vulnerability scan report in a file format other than HTML, if any. In addition to HTML, the generated vulnerability scan reports may also be available in PDF and MSWord (RTF) formats, depending on your output configuration. For more information about on setting output options, see “Configuring vulnerability scan jobs” on page 162 .
Action	Select Delete to remove the report.

To view a vulnerability scan report

- 1 Go to **Tools > Vulnerability Scan > Report**.
- 2 To view the report in HTML format, in the Job Name column, select the name of the report.
- 3 To view the report in PDF or MSWord (RTF) format, in the Formats column, select the name of the file format.

If you configured the vulnerability scan report output options to include other file formats, you can also view the report in those file formats.

Vulnerability scan reports contain results based upon port scans, software fingerprinting, and tests performed by vulnerability scan modules; the accuracy of these assessments depends on proper preparation of the network, RVS modules, and target hosts, and is subject to the limitations of the FortiAnalyzer unit's access to the target host. For more information about minimizing the number of false negative or false positive results, see [“Preparing for the vulnerability scan job” on page 157](#).

File Explorer

The File Explorer menu allows administrators to view and browse through the files on their FortiAnalyzer unit. To view and browse through these files, go to **Tools > File Explorer**.

In **Tools > File Explorer**, you can browse through what logs are stored on the FortiAnalyzer unit. The files have a two main directories: drive0/private and Storage. The Storage directory contains all information that is considered storage on the FortiAnalyzer unit, such as log files and local log files.

You can expand and hide the two main directories as well as sub-directories by selecting the plus or minus signs, located beside each main and sub-directory file name.

Figure 5: File Explorer

Name	Size(bytes)	Date Modified
aggregation	4096	Tue Aug 21 13:35:49 2007
config	4096	Mon May 26 10:50:53 2008
email_files	4096	Wed Sep 5 13:34:45 2007
etc	4096	Fri Jan 12 06:19:46 2007
ftp_files	4096	Wed Sep 5 13:34:45 2007
http_files	4096	Wed Sep 5 13:34:43 2007
im_files	4096	Wed Sep 5 13:34:45 2007
import	4096	Thu May 24 09:06:33 2007
index	4096	Mon Nov 19 00:46:57 2007
logo	4096	Mon Feb 26 10:08:39 2007
Logs	4096	Fri Jan 12 06:25:17 2007
mms_files	4096	Wed Sep 5 13:34:45 2007
quard_files	4096	Wed Sep 5 13:34:45 2007
queue	4096	Fri Jan 12 06:26:00 2007
reportlang	4096	Wed Sep 5 13:34:30 2007
sum_reports	4096	Thu May 29 08:38:14 2008
tmp	4096	Tue Nov 20 11:25:40 2007
upload_queue	4096	Tue Nov 20 11:33:01 2007
uploadd_temp	4096	Fri Oct 19 13:48:16 2007
vuln	4096	Fri Jan 12 06:25:18 2007
bin_work_done	28	Tue Nov 20 11:28:28 2007
index_work_done	28	Thu Nov 15 08:52:20 2007
drive_mounted	0	Mon Jun 2 05:53:01 2008
idx.status	283648	Thu Oct 18 13:42:16 2007
msgsys	84	Tue Nov 20 11:25:26 2007
swapfile	536809472	Tue Nov 20 11:25:23 2007

Figure 6: File Explorer with Storage directory expanded

Name	Size(bytes)	Date Modified
.self	4096	Tue Nov 20 11:33:28 2007
.sniffer	4096	Tue Nov 20 11:33:28 2007
SYSL0G-172.20.120.149	4096	Fri Mar 7 12:23:35 2008
SYSL0G-172.20.120.46	4096	Tue Mar 25 06:41:35 2008
SYSL0G-192.168.2.5	4096	Fri Mar 7 12:03:34 2008
FE-4002905500125	4096	Tue Nov 20 11:33:28 2007
FE-4002905500551	4096	Wed May 14 06:00:00 2008
FG100A2906500197	4096	Wed May 21 08:10:53 2008
FG200A2907500558	4096	Tue Nov 20 11:33:28 2007
FG30002805033034	4096	Thu Feb 14 13:18:46 2008
FG36002804033100	4096	Tue Nov 20 11:33:28 2007
FG50012204400045	4096	Tue Jan 22 08:08:45 2008
FG50012205400050	4096	Wed Jan 16 11:37:45 2008
FGT-602803030112	4096	Tue Feb 25 12:31:28 2008
FGT-602803030702	4096	Wed Feb 20 07:25:34 2008
FGT-602803031626	4096	Wed May 14 06:00:01 2008
FGT-602906512797	4096	Mon Mar 3 11:48:50 2008
FGT5002801021077	4096	Tue Nov 20 11:33:28 2007
FGT5002803033050	4096	Tue Nov 20 11:33:28 2007
FGT50B3G06500085	4096	Tue Dec 18 08:41:35 2007
FGT60B3907513142	4096	Thu Mar 13 12:03:28 2008
FGT60B3907515488	4096	Fri Mar 14 10:15:07 2008
FMG-3K2404400063	4096	Tue Nov 20 11:33:28 2007
FortiClient	4096	Tue Nov 20 11:33:28 2007
FWF60A2906501184	4096	Tue Nov 20 11:33:28 2007
jattackid.desc	9569	Sun Nov 18 22:00:14 2007
eventcode.desc	6221	Sun Nov 18 22:00:14 2007
table_a_service.db	2048	Wed Oct 17 13:30:23 2007
table_a_service.lst	16	Thu Sep 13 13:55:04 2007
table_a_status.db	2048	Wed Oct 17 13:37:04 2007
table_a_status.lst	77	Thu Sep 13 13:55:04 2007
table_a_subtype.db	2048	Wed Oct 17 13:37:04 2007
table_a_subtype.lst	19	Thu Sep 13 13:55:04 2007
table_action.db	2048	Wed Oct 17 13:40:14 2007
table_action.lst	271	Wed Oct 17 13:30:16 2007
table_agent.db	2048	Thu Sep 13 13:55:04 2007
table_agent.lst	1	Thu Sep 13 13:55:04 2007
table_atkidd.db	6144	Wed Oct 17 13:37:04 2007
table_atkidd.lst	1045	Thu Sep 13 13:55:04 2007
table_attack.db	14336	Wed Oct 17 13:37:04 2007
table_attack.lst	4884	Thu Sep 13 13:55:04 2007

Managing firmware versions

Before upgrading to FortiAnalyzer 3.0, it is recommended to review this chapter so you can be fully aware of the procedures and issues when upgrading to FortiAnalyzer 3.0. This chapter includes upgrading issues for all FortiAnalyzer 3.0 firmware versions and how to revert back to a previous firmware version, either to FortiLog 1.6 or an earlier FortiAnalyzer 3.0 firmware version.

In addition to firmware images, Fortinet releases patch releases—maintenance release builds that resolve important issues. Fortinet strongly recommends reviewing the release notes for the patch release before upgrading the firmware. Follow the steps below:

- download and review the release notes for the patch release
- download the patch release
- back up the current configuration
- install the patch release using the procedure [“Testing firmware before upgrading” on page 172](#)
- test the patch release until you are satisfied that it applies to your configuration

Installing a patch release without reviewing release notes or testing the firmware may result in changes to settings or unexpected issues.

This chapter includes the following sections:

- [Backing up your configuration](#)
- [Testing firmware before upgrading](#)
- [Upgrading your FortiAnalyzer unit](#)
- [Restoring your configuration](#)
- [Reverting to a previous firmware version](#)



Note: Fortinet recommends upgrading the FortiAnalyzer unit during a low traffic period, for example at night, to re-index log data. Generating reports before the log index is complete results in incorrect data in reports. The FortiAnalyzer unit will take time to complete the index if there is a lot of log data. You can verify that the indexing is complete by viewing the Alert Message console on the Dashboard.

Backing up your configuration

Fortinet recommends backing up all configuration settings from your FortiAnalyzer unit before upgrading to FortiAnalyzer 3.0. This ensures all configuration settings are not lost if you require downgrading to FortiLog 1.6 and want to restore those configuration settings.



Caution: Always backup your configuration before installing a patch release, upgrading/downgrading, or when resetting to factory defaults.

Always back up log data before upgrading/downgrading.

Backing up your configuration using the web-based manager

The following procedures describe how to back up your current configuration using the web-based manager.

To back up your configuration file in FortiLog 1.6 using the web-based manager

- 1 Go to **Maintenance > Backup & Restore**.
- 2 Select the Backup icon for the configuration that you want to back up.
- 3 Save the file to the local directory on the management computer.

To back up your configuration file in FortiAnalyzer 3.0 and higher using the web-based manager

- 1 Go to **System > Maintenance > Backup & Restore**.
- 2 Select Local PC from the Backup Configuration to list.
- 3 Select Apply.

If you want to encrypt your configuration file, select the Encrypt configuration file check box, enter a password, and enter the password again to confirm.

Backing up your configuration using the CLI

The following procedure describes how to backup up your current configuration using the CLI. You can enter a password, if required.

To back up your configuration file using the CLI

Enter the following to back up the configuration:

```
execute backup config <filename> <address_ip> <passwd>
```

This may take a few minutes.

Backing up your log files

Backing up your log files uses the same procedure as downloading log files. You can back up log files using either the web-based manager or CLI. Fortinet recommends backing up all log files before upgrading/downgrading, resetting to factory defaults or when testing a new firmware image.

To back up log files using the web-based manager

- 1 Go to **Log > Browse**.
- 2 In the Log Files column, locate a device and log type. Select blue arrows to expand and reveal the specific log file (`wlog.log`, `elog.log`, etc.) that you want to back up.
- 3 In the Action column, select Download for that log file's row.
- 4 Select one of the following:

Convert to CSV format

Backs up the log format as a comma-separated value (`.csv`) file instead of a standard `.log` file. Each log element is separated by a comma. CSV files can be viewed in spreadsheet applications.

Compress with gzip

Compress the `.log` or `.csv` file with gzip compression. For example, downloading a log-formatted file with gzip compression would result in a download with the file extension `.log.gz`.

- 5 Select OK.
- 6 Select a location when prompted by your web browser to save the file.

To back up log files using the CLI

Enter the following to back up all log files:

```
execute backup logs all {ftp | sftp | scp| tftp}  
<server_ipv4> <username_str> <password_str> <directory_str>
```

If you are using a TFTP server, you do not need to enter a user name, password or directory.

After successfully backing up your configuration file, either from the CLI or the web-based manager, proceed with upgrading to FortiAnalyzer 3.0.

Testing firmware before upgrading

You may want to test the firmware you want to install before upgrading to a new firmware version, maintenance or patch release. By testing the firmware image, you can familiarize yourself with the new features and changes to existing features, as well as understand how your configuration works with the firmware. You can test a firmware image by installing it from a system reboot and saving it to system memory. After the firmware is saved to system memory, the FortiAnalyzer unit operates using the firmware with the current configuration.

The procedure does not permanently install the firmware; the next time the FortiAnalyzer unit restarts, it operates using the firmware originally installed on the FortiAnalyzer unit. You can install the firmware permanently using the procedures in [“Upgrading your FortiAnalyzer unit” on page 174](#).

You can use the following procedure regardless of the type of firmware image, for example, a patch release.



Note: After you have tested the firmware, and rebooted the FortiAnalyzer unit, the original configuration does not resume. You need to restore the configuration after testing the firmware.

To test the firmware image before upgrading

- 1 Copy the new firmware image file to the root directory of the TFTP server.
- 2 Start the TFTP server.
- 3 Log into the CLI.
- 4 Enter the following command to ping the computer running the TFTP server:

```
execute ping <server_ipaddress>
```

Pinging the computer running the TFTP server verifies that the FortiAnalyzer unit and TFTP server are successfully connected.

- 5 Enter the following to restart the FortiAnalyzer unit.
- 6 As the FortiAnalyzer unit reboots, a series of system startup messages appears. When the following message appears,

```
Press any key to display configuration menu...
```

- 7 Immediately press any key to interrupt the system startup.

You have only three seconds to press any key. If you do not press a key soon enough, the FortiAnalyzer unit reboots and you must log in and repeat steps 5 to 7 again.

If you successfully interrupt the startup process, the following message appears:

```
[G]: Get firmware image from TFTP server.
```

```
[F]: Format boot device.
```

```
[B]: Boot with backup firmware and set as default.
```

```
[C]: Configuration and information.
```

```
[Q]: Quit menu and continue to boot with default firmware.
```

```
[H]: Display this list of options.
```


- 8** Type G to get the new firmware image from the TFTP server.
The following message appears:
Enter TFTP server address [192.168.1.168]:
- 9** Type the address of the TFTP server and press Enter.
The following message appears:
Enter Local Address [192.168.1.188]:
- 10** Type the internal IP address of the FortiAnalyzer unit.
This IP address connects the FortiAnalyzer unit to the TFTP server. This IP address must be on the same network as the TFTP server, but make sure you do not use an IP address of another device on the network.
The following message appears:
Enter firmware image file name [image.out]:
- 11** Enter the firmware image file name and press Enter.
The TFTP server uploads the firmware image file to the FortiAnalyzer unit and the following appears:
Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]
- 12** Type R.
The FortiAnalyzer firmware image installs and saves to system memory. The FortiAnalyzer unit starts running the new firmware image with the current configuration.
When you are done testing the firmware, you can reboot the FortiAnalyzer unit and resume using the original firmware. You will need to restore the original configuration file after the testing.

Upgrading your FortiAnalyzer unit

After backing up your current configuration, you can now upgrade the firmware on your FortiAnalyzer unit. The following procedures are used every time you are upgrading the firmware that is associated with the firmware version FortiAnalyzer 3.0, whether it is a maintenance release or patch release.

You can also use the following procedure when installing a patch release. A patch release is a maintenance release build that resolves important issues. You can install a patch release whether the FortiGate unit was upgraded to the current firmware version or not.

The following configuration settings are not carried forward when upgrading from FortiLog 1.6 to FortiAnalyzer 3.0:

- | | |
|------------------------|---|
| Alerts | <ul style="list-style-type: none"> • Destination is not carried forward in Alerts Event configuration. |
| Report profiles | <ul style="list-style-type: none"> • Report Selection is reset to all queries because of the new report types added and the report re-organization • System is not restored in the Device Selection • Output is reset to HTML file only. |
| Devices | <ul style="list-style-type: none"> • Devices defined in FortiLog 1.6 are carried forward and devices privileges set to "Allow FortiGate to send logs here" only. • Syslog privileges are also carried forward. |
| IP Aliases | <ul style="list-style-type: none"> • IP Aliases are not carried forward from FortiLog 1.6 to FortiAnalyzer 3.0. |

You need to upgrade to FortiLog 1.6 before upgrading to FortiAnalyzer 3.0. FortiAnalyzer 3.0 does not support upgrading from earlier FortiLog firmware versions.

When upgrading your FortiAnalyzer unit, Fortinet recommends upgrading to the EXT3 file system. This is done by using the `execute formatlogdisk` command in the CLI. The file system changes from Reiser to EXT3. The EXT3 file system provides better stability. You can upgrade to the EXT3 file system if upgrading to FortiAnalyzer 3.0 MR3 and higher. See the *FortiAnalyzer CLI Reference* for more information about upgrading to the EXT3 file system.

Upgrading to FortiAnalyzer 3.0

This section describes how to properly upgrade to FortiOS 3.0 and higher using either the web-based manager or CLI.

If the web-based manager and CLI are unresponsive, and the FortiAnalyzer unit cannot complete its startup, see ["Restoring your configuration" on page 180](#).

Upgrading using the web-based manager

The following procedure uses the web-based manager for upgrading to FortiAnalyzer 3.0.



Caution: Always backup your configuration before installing a patch release, upgrading/downgrading, or when resetting to factory defaults.

Always back up log data before upgrading/downgrading.

To upgrade to FortiAnalyzer 3.0 using the web-based manager

- 1 Copy the firmware image file to your management computer.
- 2 Log into the web-based manager as the administrative user.
- 3 Go to **System > Dashboard**.
- 4 In the System Information area, select Update.
- 5 Enter the path and filename of the firmware image file, or select Browse and locate the file.
- 6 Select OK.
- 7 Update AV/NIDS definitions so that they are current with the new firmware.

The FortiAnalyzer unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiAnalyzer login. This process may take a few minutes.

When the upgrade is successfully installed:

- Ping to your FortiAnalyzer unit to verify there is still a connection.
- Clear the browser's cache and log into the web-based manager.

After logging back into the web-based manager, you should save the configuration settings that carried forward. Some settings may have carried forward from FortiLog 1.6, while others may not have such as the Destination in Alerts Event configuration. Go to **System > Maintenance > Backup & Restore** to save the configuration settings that carried forward.

Upgrading using the CLI

The following procedure uses the CLI to upgrade to FortiAnalyzer 3.0 and a TFTP server. The CLI upgrade procedure reverts all current firewall configurations to factory default settings.

To upgrade to FortiAnalyzer 3.0 using the CLI

- 1 Copy the new firmware image file to the root directory of the TFTP server.
- 2 Start the TFTP server.
- 3 Log into the CLI.
- 4 Enter the following command to ping the computer running the TFTP server:

```
execute ping <server_ipaddress>
```

Pinging the computer running the TFTP server verifies that the FortiAnalyzer unit and TFTP server are successfully connected.

- 5 Enter the following command to copy the firmware image from the TFTP server to the FortiAnalyzer unit:

```
execute restore image <name_str> <tftp_ip4>
```

When `<name_str>` is the name of the firmware image file and `<tftp_ip>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is `192.168.1.168`, enter:

```
execute restore image.out 192.168.1.168
```

The FortiAnalyzer unit responds with a message similar to the following:

```
This operation will replace the current firmware version!  
Do you want to continue? (y/n)
```

6 Type `y`.

The FortiAnalyzer unit uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.

7 Reconnect to the CLI.

8 Enter the following command syntax to confirm the firmware image installed successfully:

```
get system status
```

9 Update AV/NIDS definitions so that they are current with the new firmware.

Verifying the upgrade

After logging back into the web-based manager, most of your FortiLog 1.6 configuration settings have been carried forward.

You should verify what configuration settings carried forward. You should also verify that administrative access settings carried forward as well. Verifying your configuration settings enables you to familiarize yourself with the new features and changes in FortiAnalyzer 3.0.

You can verify your configuration settings by:

- going through each menu and tab in the web-based manager
- using the `show` shell command in the CLI

Reverting to a previous firmware version

You may need to revert to a previous firmware version if the upgrade did not install successfully. The following sections will help you to backup your current FortiAnalyzer 3.0 configuration, downgrade to FortiLog 1.6, and restore your FortiLog 1.6 configuration.

The following topics are included in this section:

- [Backing up your configuration using the web-based manager](#)
- [Downgrading to FortiLog 1.6](#)
- [Restoring your configuration](#)

You can use the procedure, “[To back up your configuration file in FortiAnalyzer 3.0 and higher using the web-based manager](#)” on page 170 to back up your FortiAnalyzer 3.0 configuration. Fortinet recommends backing up your configuration file when upgrading, downgrading, reverting to factory defaults, or installing a patch release.

Downgrading to FortiLog 1.6

When downgrading to FortiLog 1.6, no settings are carried forward. If you created additional settings in FortiAnalyzer 3.0, make sure to back up the current configuration before downgrading. See “[Backing up your configuration](#)” on page 169 for more information.

To downgrade using the web-based manager

- 1 Go to **System > Status > Firmware Version**.
- 2 Select Update.
- 3 Type the location of the firmware version or select Browse.
- 4 Select OK.

The following message appears:

```
The new image does not support CC mode. Do you want to
continue to upgrade?
```

- 5 Select OK.

The following message appears:

```
This version will downgrade the current firmware version.
Are you sure you want to continue?
```

- 6 Select OK.

The FortiAnalyzer unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiAnalyzer login. This process takes a few minutes.

- 7 Log into the web-based manager.

Go to **System > Dashboard > System Information** to verify the Firmware Version has changed to FortiLog 1.6.

Verifying the downgrade

After successfully downgrading to FortiLog 1.6, verify your connections and settings. If you are unable to connect to the web-based manager, make sure your administration access settings and internal network IP address are correct. The downgrade may change your configuration settings to default settings.

Downgrading to FortiLog 1.6 using the CLI

The following procedure enables you to downgrade to FortiLog 1.6 in the CLI. If you have created additional settings in FortiAnalyzer 3.0, make sure you back up your configuration before downgrading. See [“Backing up your configuration” on page 169](#) for more information.

To downgrade using the CLI

- 1 Copy the new firmware image file to the root directory of the TFTP server.
- 2 Start the TFTP server.
- 3 Log into the CLI.
- 4 Enter the following command to ping the computer running the TFTP server:

```
execute ping <server_ipaddress>
```

Pinging the computer running the TFTP server verifies that the FortiAnalyzer unit and TFTP server are successfully connected.

- 5 Enter the following command to copy the firmware image from the TFTP server to the FortiAnalyzer unit:

```
execute restore image tftp <name_str> <tftp_ipv4>
```

Where `<name_str>` is the name of the firmware image file and `<tftp_ipv4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is `192.168.1.168`, enter:

```
execute restore image tftp image.out
192.168.1.168
```

The FortiAnalyzer unit responds with the message:

```
This operation will replace the current firmware version! Do
you want to continue? (y/n)
```

- 6 Type `y`.

The FortiAnalyzer unit uploads the firmware image file. After the file uploads, a message similar to the following is displayed:

```
Get image from tftp server OK.
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```

- 7 Type `y`.

The FortiAnalyzer unit reverts to the old firmware version, resets the configuration to factory defaults, and restarts. This process takes a few minutes.

After the FortiAnalyzer unit uploads the firmware, you need to reconfigure your IP address since the FortiAnalyzer unit reverts to default settings, including its default IP address. See your install guide for configuring IP addresses.

- 8 Reconnect to the CLI.
- 9 Enter the following command to confirm the firmware image installed successfully:

```
get system status
```

See [“Restoring your configuration” on page 180](#) to restore you FortiLog 1.6 configuration settings.

Restoring your configuration

Your configuration settings may not carry forward after downgrading to FortiLog 1.6. You can restore your configuration settings for FortiLog 1.6 with the configuration file(s) you saved before upgrading to FortiAnalyzer 3.0.

During a firmware restoration, the TFTP server IP address must be on the same network as the FortiAnalyzer unit's IP address: the FortiAnalyzer unit uses a 255.255.255.0 net mask when connecting to a TFTP server for firmware. For this reason, instead of temporarily reconfiguring the rest of the network, it may be more convenient to install a TFTP server on your management computer and create a temporary peer network with the FortiAnalyzer unit, connecting it directly to the TFTP server on your management computer.

You can also use the following procedures for restoring your configuration after installing a patch release.

Restoring configuration settings on a FortiAnalyzer unit

You can restore configuration settings whether the FortiAnalyzer unit was downgraded, reset to factory defaults, or may be corrupted. Use the recovery procedure appropriate for your FortiAnalyzer unit model to restore the firmware from a TFTP server.

For more information about connecting to the CLI, see the [FortiAnalyzer CLI Reference](#).

Restoring the firmware also restores the default configuration for that firmware version. The following restores a FortiAnalyzer-100A/100B, FortiAnalyzer-800/800B, FortiAnalyzer-2000/2000A, and FortiAnalyzer-4000/4000A



Note: When connecting the Ethernet cable to the FortiAnalyzer-800, insert the cable into the LAN2 port.

To restore a firmware image to the FortiAnalyzer unit

- 1 Copy the new firmware image file to the root directory of the TFTP server.
- 2 Start the TFTP server.
- 3 Log into the CLI.
- 4 Enter the following command to ping the computer running the TFTP server:

```
execute ping <server_ipaddress>
```

Pinging the computer running the TFTP server verifies that the FortiAnalyzer unit and TFTP server are successfully connected. If you enabled firewalls, such as Windows Firewall, you will need to modify them because they interfere when connecting to the TFTP server.

- 5 If the CLI is *not* responsive, power cycle the FortiAnalyzer unit to reboot.
If the CLI is responsive, enter the following command to restart the FortiAnalyzer unit:

```
execute reboot
```

As the FortiAnalyzer unit starts, a series of system startup messages are displayed.

6 When this message appears:

Press any key to display configuration menu...

immediately press a key to interrupt the system startup.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
```

Enter G, F, B, Q, or H:

7 Type G to get the new firmware image from the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

8 Type the address of the TFTP server and press Enter.

The following message appears:

```
Enter Local Address [192.168.1.188]:
```

9 Type an IP address for the FortiAnalyzer unit and press Enter.

The FortiAnalyzer unit will temporarily assign this IP address to the interface to connect to the TFTP server and download the firmware.

This IP address can be any IP address that is valid for the network the interface is connected to, as long as it does not conflict with another device on this network.

The following message appears:

```
Enter File Name [image.out]:
```

10 Type the firmware image file name and press Enter.

The TFTP server uploads the firmware image file to the FortiAnalyzer unit. The CLI displays messages as it downloads and verifies the firmware image:

```
MAC:00090F601129
#####
Total 17268465 bytes data downloaded.
Verifying the integrity of the firmware image.

Total 28000kB unzipped.
```

When the upload is complete, the CLI displays the following message:

```
Save as Default firmware/Backup firmware/Run image without
saving:[D/B/R]
```

11 Type D.

The FortiAnalyzer unit installs the new firmware image and restarts.

Restoring your configuration settings using the web-based manager

The following restores your FortiLog 1.6 configuration settings using the web-based manager.

To restore configuration settings using the web-based manager

- 1 Log into the web-based manager.
- 2 Go to **System > Maintenance > Backup & Restore**.
- 3 Select the Restore icon for All Configuration Files.
- 4 If required, enter your password for the configuration file.
- 5 Type the location of the file or select Browse to locate the file.
- 6 Select OK.

The FortiAnalyzer unit restores the configuration settings for FortiLog 1.6. This may take a few minutes since the FortiAnalyzer unit will reboot.

You can verify that the configuration settings are restored by logging into the web-based manager and going through the various menus and tabs.

Restoring your configuration settings using the CLI

The following restores your FortiLog 1.6 configurations settings using the CLI.

To restore configuration settings using the CLI

- 1 Copy the backup configuration file to the root directory of the TFTP server.
- 2 Start the TFTP server.
- 3 Log into the CLI.
- 4 Enter the following command to ping the computer running the TFTP server:

```
execute ping <server_ipaddress>
```

Pinging the computer running the TFTP server verifies that the FortiAnalyzer unit and TFTP server are successfully connected.

- 5 Enter the following command to copy the backup configuration file to restore the file on the FortiAnalyzer unit:

```
execute restore config <name_str> <tftp_ipv4> <passwd>
```

Where `<name_str>` is the name of the backup configuration file and `<tftp_ipv4>` is the IP address of the TFTP server and `<passwd>` is the password you entered when you backup your configuration settings. For example, if the backup configuration file is `confall` and the IP address of the TFTP server is `192.168.1.168` and the password is `ghrffdt123`:

```
execute restore config confall 192.168.1.168 ghrffdt123
```

The FortiAnalyzer unit responds with the message:

```
This operation will overwrite the current settings!
Do you want to continue? (y/n)
```

6 Type `y`.

The FortiAnalyzer unit uploads the backup configuration file. After the file uploads, a message, similar to the following, is displayed:

```
Getting file confall from tftp server 192.168.1.168
##
Restoring files...
All done. Rebooting...
```

This may take a few minutes.

Use the `show shell` command to verify your settings are restored, or log into the web-based manager.

Appendix: FortiAnalyzer reports in 3.0 MR7

Reports have changed dramatically in FortiAnalyzer 3.0 MR7, from how you configure them to the default naming scheme given when generated. Fortinet recommends reviewing the *FortiAnalyzer Administration Guide* for FortiAnalyzer 3.0 MR7 to help you understand and familiarize yourself with the changes.

The following explains the changes that occurred with the available reports that you can choose when configuring reports.

This section includes the following topics:

- [FortiGate reports](#)
- [Summary Reports](#)
- [Forensic Reports](#)
- [FortiMail Reports](#)
- [FortiClient Reports](#)

FortiGate reports

The FortiGate reports changed in FortiAnalyzer 3.0 MR7. The following explains what reports were renamed, removed, or unchanged.

FortiGate reports include:

- [Intrusion Activity](#)
- [Antivirus Activity](#)
- [Webfilter Activity](#)
- [Antispam Activity](#)
- [IM Activity](#)
- [VoIP reports](#)
- [Content Activity](#)
- [Network Activity](#)
- [Web Activity](#)
- [Mail Activity](#)
- [FTP Activity](#)
- [Terminal Activity](#)
- [VPN Activity](#)
- [Event Activity](#)
- [P2P Activity](#)
- [Audit Activity](#)

Intrusion Activity

The following table explains what Intrusion Activity reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 10: Intrusion Activity reports

MR6 reports	MR7 reports
Attacks by Direction and Type	Top Attacks per Traffic Direction
Attacks by Direction and Source	Top Attack Sources per Traffic Direction
Top Attack Types by Date	Top Attacks by Time Period
Top Attack Types by Month	Top Attacks
Top Attack Types by Day of Week	Top Attacks
Top Attack Types by Hour of Day	Top Attacks
Top Attack Types	Top Attacks
Top Attack Types by Device	Top Devices by Number of Attack Detections for Most Common Attacks
Top Attack Destinations by Type	Top Attacks for Most Common Destinations
Top Attack Destinations by Source	Top Sources for Most Common Destinations
Top Attack Types by Source	Top Sources for Most Common Attacks
Top Attacked Devices by Type	Top Attacks per Device
Attack Categories by Type	Top Attacks per Category (Signature/Anomaly)
Attacks Statuses by Type	Top Attacks per Counter-Measure
Attacks by Date	Top Attacks by Time Period
Top Attacked Destinations	Top Attacks Destinations
Top Attack Protocols by Type	Top Attack Protocols
Top Attacked Destinations by Type	Top Attacks for Most Common Destinations
Top Attack for Most Common Destinations	Top Attack Protocols

The FortiAnalyzer 3.0 MR6 report, Top Attack Sources, did not changed in FortiAnalyzer 3.0 MR7.

Antivirus Activity

The following table explains what Antivirus Activity reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 11: Antivirus Activity reports

MR6 reports	MR7 reports
Top Viruses for each Direction	Top Viruses per Traffic Direction
Top Virus Sources for each Direction	Top Virus Sources per Traffic Direction
Top Viruses by Date	Top Viruses
Top Viruses by Month	Top Viruses
Top Viruses by Day of Week	Top Viruses
Top Viruses by Hour of Day	Top Viruses
Top Virus Sources by Virus Name	Top Viruses for Most Common Sources (IP)
Top Virus Destinations by Virus Name	Top Viruses for Most Common Destinations (IP)

Table 11: Antivirus Activity reports

Top Infected Files by Date	Top Infected Files
Top Infected Files by Month	Top Infected Files
Top Infected Files by Day of Week	Top Infected Files
Top Infected Files by Hour of Day	Top Infected Files
Top Virus Sources by File Name	Top Infected Files for Most Common Sources (IP)
Top Virus Destinations by File Name	Top Infected Files for Most Common Sources (IP)
Total AV Events by Type and Date	Antivirus Violations Breakdown (Infected/Oversize/Filename)
Total AV Events by Type and Month	Antivirus Violations Breakdown (Infected/Oversize/Filename)
Total AV Events by Type and Day of Week	Antivirus Violations Breakdown (Infected/Oversize/Filename)
Total AV Events by Type and Hour of Day	Antivirus Violations Breakdown (Infected/Oversize/Filename)
Total AV Events by Type and Hour of Day	Antivirus Violations Breakdown (Infected/Oversize/Filename)
Total AV Events by Device and Type	Top Devices with Antivirus Violations Breakdown (Infected/Oversize/Filename)
Total AV Events by Service and Type	Top Protocols with Antivirus Violations Breakdown (Infected/Oversize/Filename)
Top AV Event Senders by Type	Top Sources (Email or IP) with Antivirus Violations Breakdown (Infected/Oversize/Filename)
Top AV Event Receivers by Type	Top Destination (Email or IP) with Antivirus Violations Breakdown (Infected/Oversize/Filename)
Top AV Event Sources by Type	Top Sources (IP) with Antivirus Violations Breakdown (Infected/Oversize/Filename)
Top AV Event Destinations by Type	Top Destinations (IP) with Antivirus Violations Breakdown (Infected/Oversize/Filename)
Top Infected File Extensions by Month	Top Infected File Extensions
Top Virus Sources by Hour of Day	Top Infected File Extensions
Top Virus Sources by Date	Top Virus Sources
Top Virus Sources by Month	Top Virus Sources
Top Virus Destinations by Hour of Day	Top Virus Destinations
Top Virus Destinations by Date	Top Virus Destinations
Top Virus Destinations by Month	Top Virus Destinations
Top Infected File Extensions over IMAP by Month	Top Infected File Extensions over IMAP
Top Virus Sources over IMAP by Hour of Day	Top Virus Sources over IMAP
Top Virus Sources over IMAP by Date	Top Virus Sources over IMAP
Top Virus Sources over IMAP by Month	Top Virus Sources over IMAP
Top Virus Destinations over IMAP by Hour of Day	Top Virus Destinations over IMAP

Table 11: Antivirus Activity reports

Top Virus Destinations over IMAP by Date	Top Virus Destinations over IMAP
Top Virus Destinations over IMAP by Month	Top Virus Destinations over IMAP
Top Infected File Extensions over POP3 by Month	Top Infected File Extensions over POP3
Top Virus Sources over POP3 by Hour of Day	Top Virus Sources over POP3
Top Virus Sources over POP3 by Date	Top Virus Sources over POP3
Top Virus Sources over POP3 by Month	Top Virus Sources over POP3
Top Virus Destinations over POP3 by Hour of Day	Top Virus Destinations over POP3
Top Virus Destinations over POP3 by Date	Top Virus Destinations over POP3
Top Virus Destinations over POP3 by Month	Top Virus Destinations over POP3
Top Infected File Extensions over FTP by Month	Top Infected File Extensions over FTP
Top Virus Sources over FTP by Hour of Day	Top Virus Sources over FTP
Top Virus Sources over FTP by Date	Top Virus Sources over FTP
Top Virus Sources over FTP by Month	Top Virus Sources over FTP
Top Virus Destinations over FTP by Hour of Day	Top Virus Destinations over FTP
Top Virus Destinations over FTP by Date	Top Virus Destinations over FTP
Top Virus Destinations over FTP by Month	Top Virus Destinations over FTP
Top Infected File Extensions over HTTP by Month	Top Infected File Extensions over HTTP
Top Virus Sources over HTTP by Hour of Day	Top Virus Sources over HTTP
Top Virus Sources over HTTP by Date	Top Virus Sources over HTTP
Top Virus Sources over HTTP by Month	Top Virus Sources over HTTP
Top Virus Destinations over HTTP by Hour of Day	Top Virus Destinations over HTTP
Top Virus Destinations over HTTP by Date	Top Virus Destinations over HTTP
Top Virus Destinations over HTTP by Month	Top Virus Destinations over HTTP
Top Infected File Extensions over SMTP by Month	Top Infected File Extensions over SMTP
Top Virus Sources over SMTP by Hour of Day	Top Virus Sources over SMTP
Top Virus Sources over SMTP by Date	Top Virus Sources over SMTP

Table 11: Antivirus Activity reports

Top Virus Sources over SMTP by Month	Top Virus Sources over SMTP
Top Virus Destinations over SMTP by Hour of Day	Top Virus Destinations over SMTP
Top Virus Destinations over SMTP by Date	Top Virus Destinations over SMTP
Top Virus Destinations over SMTP by Month	Top Virus Destinations over SMTP
Top Virus Senders by Virus Name	Top Viruses for Most Common Sources (Email or IP)
Top Virus Protocols by Date	Top Virus Protocols

The following reports were removed:

- Top Virus Agents by Virus Name
- Top Virus Receivers over HTTP

The following reports are unchanged:

- Top Viruses
- Top Infected Files

Webfilter Activity

The following table explains what WebFilter Activity reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 12: WebFilter Activity reports

MR6 reports	MR7 reports
Web Hits by Status	Total Hits per Status (allowed/blocked/etc)
Blocked Web Hits by Date	Blocked Web Activity over Time Period
Blocked Web Hits by Month	Blocked Web Activity over Time Period
Blocked Web Hits by Day of Week	Blocked Web Activity over Time Period
Blocked Web Hits by Hour of Day	Blocked Web Activity over Time Period
Top Web Request Destinations by Date	Top Requested Web Domains
Top Web Request Destinations by Month	Top Requested Web Domains
Top Web Request Destinations by Day of Week	Top Requested Web Domains
Top Web Request Destinations by Hour of Day	Top Requested Web Domains
Top Requested Web Pages by Date (Hits)	Top Requested Web Pages
Top Requested Web Pages by Month (Hits)	Top Requested Web Pages
Top Requested Web Pages by Day of Week (Hits)	Top Requested Web Pages
Top Requested Web Pages by Hour of Day (Hits)	Top Requested Web Pages
Web Hits for each Status by Date	Total Hits per Status (allowed/blocked/etc)
Web Hits for each Status by Month	Total Hits per Status (allowed/blocked/etc)

Table 12: WebFilter Activity reports

Web Hits for each Status by Day of Week	Total Hits per Status (allowed/blocked/etc)
Web Hits for each Status by Hour of Day	Total Hits per Status (allowed/blocked/etc)
Top Web Sources for each Device (Hits)	Top Web Users per Device
Top Web Sources by Status (Hits)	Top Web Users with Status Breakdown (allowed/blocked/etc)
Top Web Sites by Status (Hits)	Top Web Sites with Status Breakdown (allowed/blocked/etc)
Top Web Pages by Status (Hits)	Top Web Pages with Status Breakdown (allowed/blocked/etc)
Top Blocked Categories (Hits)	Top Blocked Categories
Top Requested Categories (Hits)	Top Requested Categories
Top Allowed Categories (Hits)	Top Allowed Categories
Web Hits by Filter Type	Total Hits per Web Filter Type
Top Blocked Web Risk Groups (Hits)	Top Blocked Web Risk Groups
Top Web Risk Groups (Hits)	Top Requested Web Risk Groups
Top Web Clients by Web Site (Hits)	Top Web Sites for Most Active Users
Top Blocked Web Clients by Web Site (Hits)	Top Web Sites for Most Blocked Users
Top Web Clients (Hits)	Top Active Web Users
Top Web Clients by Web Site and Category (Hits)	Top Web Sites+Category for Most Active Users
Allowed Web Hits by Hour	Allowed Web Activity over Time Period
Allowed Web Hits by Date	Allowed Web Activity over Time Period
Allowed Web Hits by Month	Allowed Web Activity over Time Period
Top Allowed Web Sources (Hits)	Top Allowed Web Users
Top Blocked Web Sources by Category (Hits)	Top Blocked Categories for Most Active Blocked Users
Top Allowed Web Sources by Category (Hits)	Top Allowed Categories for Most Active Users
Top Overridden Web Sites (Hits)	Top Web Overrides
Top Web Sources to Overridden Web Sites (Hits)	Top Users for Web Overrides

Antispam Activity

The following table explains what Antispam Activity reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 13: Antispam Activity reports

MR6 reports	MR7 reports
Top Spammers for each Device	Top Spam Sources per Device
Top Spam Receivers for each Device	Top Spam Destinations per Device
Top Spam Blocking Criteria for each Device	Top Spam Blocking Criteria per Device

Table 13: Antispam Activity reports

Top Spammers by Blocking Criteria	Top Spam Sources with Blocking Criteria Breakdown
Top Spam Receivers by Sender	Top Spam Sources for Most Common Destinations
Mail Traffic by Status and Date	Mail Summary (by Email Size)
Mail Count Status and Date	Mail Summary (by Email Count)

The following reports are unchanged:

- Top Spam Sources
- Top Spam Destinations

The following reports were removed:

- Top Spammers Senders by Date
- Top Spammers by Month
- Top Spammers by Day of Week
- Top Spammers by Hour of Day
- Top Spammers
- Top Spammers by Blocking Criteria
- Top Spam Receivers
- Top Spam Receivers by Blocking Criteria

IM Activity

The following table explains what IM reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 14: IM reports

MR6 reports	MR7 reports
IM Activity by Action and Date	Total IM Events per Message Category (chart/file/etc)
IM activity by Action and Month	Total IM Events per Message Category (chat/file/etc)
IM Activity by Action and Day of Week	Total IM Events per Message Category (chat/file/etc)
IM Activity by Action and Hour of Day	Total IM Events per Message Category (chat/file/etc)
Top Allowed Local IM Users by Date	Top Allowed Local IM Users
Top Allowed Local IM Users by Month	Top Allowed Local IM Users
Top Blocked Local IM Users by Date	Top Blocked Local IM Users
Top Blocked Local IM Users by Month	Top Blocked Local IM users
Top Allowed Remote IM users by Date	Top Allowed Remote IM Users
Top Allowed Remote IM Users by Month	Top Allowed Remote IM Users
Top Blocked Remote IM Users by Date	Top Blocked Remote IM Users

Table 14: IM reports

Top Blocked Remote IM Users by Month	Top Blocked Remote IM Users
Top Local IM Users by Date	Top Local IM Users
Top Local IM users by Month	Top Local IM Users
Top Local IM users by Action	Top Local IM Users per Message Category (chat/file/ect)
IM Activity by Protocol	Total IM Events per Protocol
Top Allowed Local IM Users for each Protocol	Top Allowed Local IM Users per IM protocol
Top BLocked Local IM Users for each Protocol	Top Blocked Local IM Users per IM Protocol

VoIP reports

The following table contains the new VoIP reports that are available in FortiAnalyzer 3.0 MR7.

Table 15: VoIP reports

MR7 reports
VoIP Traffic by Date
VoIP Traffic by Month
VoIP Traffic by Day of Week
VoIP Traffic by Hour of Day
VoIP Traffic by Direction
Top VoIP Sources (Connections)
Top VoIP Sources (Traffic)
Top VoIP Destinations (Connections)
Top VoIP Destinations (Traffic)
Top Blocked SIP Users by Date
Top Blocked SIP Users by Month
Top Blocked SIP Users by Day of Week
Top Blocked SIP Users by Hour of Day
Top Blocked SIP Users by Reason
Top Blocked SIP Callers by Date
Top Blocked SIP Callers by Month
Top Blocked SIP Callers by Day of Week
Top Blocked SIP Callers by Hour of Day
Top Blocked SIP Callers by Reason
Top Blocked SCCP Users by Date
Top Blocked SCCP Users by Month
Top Blocked SCCP Users by Day of Week
Top Blocked SCCP Users by Hour of Day
Top Blocked SCCP Users by Reason
Top Blocked SCCP Callers by Date
Top Blocked SCCP Callers by Month

Table 15: VoIP reports

Top Blocked SCCP Callers by Day of Week
Top Blocked SCCP Callers by Hour of Day
Top Blocked SCCP Callers by Reason
VoIP Activity by Protocol
VoIP Activity by Action and Date
VoIP Activity by Action and Month
VoIP Activity by Action and Day of Week
SIP Calls by Status
SIP Call Registered by Date
SIP Call Registers by Month
SIP Call Registers by Day of Week
SIP Call Registers by Hour of Day
SIP Call Durations
Top SIP Called Numbers by Date
Top SIP Called Numbers by Month
Top SIP Called Numbers by Day of Week
Top SIP Called Numbers by Hour of Day
Top SIP Users (Number of Calls)
Top SIP Users (Duration)
SCCP Calls by Status
SCCP Call Registers by Date
SCCP Call Registers by Date
SCCP Call Registers by Month
SCCP call Registers by Day of Week
SCCP Call Registers by Hour of Day
SCCP Call Durations
Top SCCP Called Numbers by Date
Top SCCP Called Numbers by Month
Top SCCP Called Numbers by Day of Week
Top SCCP Called NUmbers by Hour of Day
Top SCCP Users (Number of Calls)
Top SCCP Users (Number of Calls)
Top SCCP Users (Duration)
Top SIP Callers by Called Numbers
Top SCCP Callers by Called Numbers

Content Activity

The following table explains what Content Activity reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 16: Content Activity reports

MR6 reports	MR7 reports
Units of Filtered Content by Service and Hour of Day	Volume of Filtered Content per Application
Units of Filtered Content by Service and Date	Volume of Filtered Content per Application
Units of Filtered Content by Service and Week	Volume of Filtered Content per Application
Units of Filtered Content by Service and Month	Volume of Filtered Content per Application
Volume of Filtered Content by Service and Hour of Day	Number of Inspected Messages per Application
Volume of Filtered Content by Service and Date	Number of Inspected Messages per Application
Volume of Filtered Content by Service and Week	Number of Inspected Messages per Application
Volume of Filtered Content by Service and Month	Number of Inspected Messages per Application

Network Activity

The following table explains what Network Activity reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 17: Network Activity reports

MR6 reports	MR7 reports
Traffic Volume by Direction and Date	Traffic Volume by Direction
Traffic Volume by Direction and Month	Traffic Volume by Direction
Traffic Volume by Direction and Day of Week	Traffic Volume by Direction
Traffic Volume by Direction and Hour of Day	Traffic Volume by Direction
Top Traffic Volumes by Service and Direction	Top Services by Volume per Traffic Direction
Top Traffic Volumes by Source	Top Sources by Volume
Top Traffic Volumes by Source and Service	Top Services by Volume for most Common Sources.
Top Traffic Volumes by Source and Destination	Top Source Destination Pairs by Volume
Top Traffic Volumes by Destination	Top Destinations by Volume
Top Traffic Volumes by Destination and Service	Top Services by Volume for most Common Destinations
Top Traffic Volumes by Destination and Source	Top Destination-Source Pairs by Volume
Top Traffic Durations by Destination	Top Destinations by Firewall Session Duration
Top Traffic Durations by Source	Top Sources by Firewall Session Duration
Top Traffic Durations by Client	Top Users by Firewall Session Duration
Top Traffic Durations by Group	Top User Groups by Firewall Session Duration

Table 17: Network Activity reports

Top Traffic Volumes by Service	Top Services by Volume
Traffic Volume of each Device by Date	Traffic Volume by Direction

The following reports are unchanged:

- Traffic Volume by Direction
- Top Denied Policies
- Top Denied Services
- Top Denied Sources
- Top Denied Destinations

Web Activity

The following table explains what Web Activity reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7. This table also includes the category that the reports were moved to, if applicable.

Table 18: Web Activity reports

MR6 reports	MR7 reports	Category that reports were moved to in MR7 (if applicable)
Web Traffic by Date	Web Volume by Time Period	
Web Traffic by Month	Web Volume by Time Period	
Web Traffic by Day of Week	Web Volume by Time Period	
Web Traffic by Hour of Day	Web Volume by Time Period	
Web Traffic by Direction	Web Volume per Traffic Direction	
Top Web Sites (Connections)	Top Web Servers by Connections	
Top Web Sites (Traffic)	Top Web Servers by Volume	
Top Web Sites (Traffic+Hits)	Top Web Servers by Volume and Hits	
Top Web Pages by Client (Hits)	Top Users for Most Requested Web Pages	Web Filter Activity
Top Web Clients (Connections)	Top Web Clients by Connections	
Top Web Clients (Traffic)	Top Web Clients by Volume	
Top Web Clients by Web Site (Connections)	Top Web Servers by Connections for most Active Clients	
Top Web Clients by Web Site (Traffic)	Top Web Servers by Volume for most Active Clients	
Web Traffic by Top Web Servers	Top HTTP Servers by Volume	Content Activity
Web Traffic by Status and Top Web Servers	Top HTTP Servers by Volume	Content Activity
Top Web Sites (Duration)	Top Web Servers by Firewall Session Duration	

Table 18: Web Activity reports

Top Web Clients (Duration)	Top Web Clients by Firewall Session Duration	
Top Web Clients by Web Sites (Duration)	Top Web Servers by Firewall Session Duration for most Active Clients	

The following reports were removed:

- Top Web Pages (Hits)
- Top Web Pages (Traffic)
- Top Web Clients (Browse Time)
- Top Web Users (Browse Time)

Mail Activity

The following table explains what Mail Activity reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 19: Mail Activity reports

MR6 reports	MR7 reports
Mail Traffic by Date	Mail Volume/Size by Time
Mail Traffic by Month	Mail Volume/Size by Time
Mail Traffic by Day of Week	Mail Volume/Size by Time
Mail Traffic by Hour by Day	Mail Volume/Size by Time
Mail Traffic by Direction	Mail Volume/Size by Traffic Direction
Top Mail Servers (Traffic)	Top Mail Servers (by Volume)
Top Mail Clients (Traffic)	Top Mail Clients (by Volume)
Top Mail Servers by Clients (Connections)	Top Mail Clients for Most Common Mail Servers (Connections)
Top Mail Servers by Clients (Traffic)	Top Mail Clients for Most Common Mail Servers (by Volume)
Mail Traffic by Service and Sender	Top Sender by Volume for each Mail Protocol
Mail Traffic by Service and Receiver	Top Receiver by Volume for each Mail Protocol
Mail Traffic by Status and Sender	Top Mail Sources for each Spam Detection Status (clean/spam/etc)
Mail Traffic by Status and Receiver	Top Mail Destination for each Spam Detection Status (clean/spam/etc)

The report, Top Mail Servers (Connections) remains unchanged.

FTP Activity

The following table explains what FTP Activity reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 20: FTP Activity reports

MR6 reports	MR7 reports
FTP Traffic by Date	FTP Volume by Time Period
FTP Traffic by Month	FTP Volume by Time Period
FTP Traffic by Day of Week	FTP Volume by Time Period

Table 20: FTP Activity reports

FTP Traffic by Hour of Day	FTP Volume by Time Period
FTP Traffic by Direction	FTP Volume per Traffic Direction
Top FTP Sites (Connection)	Top FTP Servers by Connections
Top FTP Sites (Traffic)	Top FTP Servers by Volume
Top FTP Clients (Connection)	Top FTP Clients by Connections
Top FTP Clients (Traffic)	Top FTP Clients by Volume
Top FTP Clients by FTP Server (Connections)	Top Client-Server Pairs by Connections
Top FTP Clients by FTP Server (Traffic)	Top Client-Server Pairs by Volume

Terminal Activity

The following table explains what Terminal Activity reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 21: Terminal Activity reports

MR6 reports	MR7 reports
Terminal Traffic by Service and Date	Terminal Traffic Volume per Service (Telnet+SSH)
Terminal Traffic by Service and Month	Terminal Traffic Volume per Service (Telnet+SSH)
Terminal Traffic by Service and Day of Week	Terminal Traffic Volume per Service (Telnet+SSH)
Terminal Traffic by Service and Hour of Day	Terminal Traffic Volume per Service (Telnet+SSH)
Telnet Traffic by Direction	Telnet Traffic Volume per Direction
SSH Traffic by Direction	SSH Traffic Volume per Direction
Top Terminal Servers by Service (Connections)	Top Terminal Servers by Connections (per Service)
Top Terminal Servers by Service (Traffic)	Top Terminal Servers by Traffic Volume (per Service)
Top Terminal Clients by Service (Connections)	Top Terminal Clients by Connections (per Service)
Top Terminal Clients by Service (Traffic)	Top Terminal Clients by Traffic Volume (per Service)
Top Telnet Clients by Server (Connections)	Top Telnet Servers by Connections for Most Active Clients
Top Telnet Clients by Server (Traffic)	Top Telnet Servers by Traffic Volume for Most Active Clients
Top SSH Clients by Server (Connections)	Top SSH Servers by Connections for Most Active Clients
Top SSH Clients by Server (Traffic)	Top SSH Servers by Traffic Volume for Most Active Clients

VPN Activity

The following table explains what VPN Activity reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 22: VPN Activity reports

MR6 reports	MR7 reports
VPN Traffic by Direction and Date	VPN Traffic Volume per Direction
VPN Traffic by Direction and Month	VPN Traffic Volume per Direction
VPN Traffic Direction Day of Week	VPN Traffic Volume per Direction
VPN Traffic by Direction and Hour of Day	VPN Traffic Volume per Direction
VPN Tunnels by Device	Total VPN Tunnels per Device
VPN Traffic by Device	VPN Traffic Volume per Device
VPN Tunnels by Device and Peer	Top VPN Peers per Device (by Number of Tunnels)
VPN Traffic by Device and Peer	Top VPN Peers per Device (by Traffic Volume)
VPN Traffic by Device and Service	Top Protocols over VPN per Device (by Traffic Volume)
Top VPN Traffic Sources	Top VPN Sources
Top VPN Traffic Destinations	Top VPN Destinations
VPN Traffic by Direction	VPN Traffic Volume per Direction
Top VPN Tunnels Date (Traffic)	Top VPN Tunnels
Top VPN Tunnels by Month (Traffic)	Top VPN Tunnels
Top VPN Tunnels by Day of Week (Traffic)	Top VPN Tunnels
Top VPN Tunnels by Hour of Day (Traffic)	Top VPN Tunnels
Top VPN Tunnels (Traffic)	Top VPN Tunnels

Event Activity

The following table explains what Event Activity reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 23: Event Activity reports

MR6 reports	MR7 reports
Top Events	Top Events (by Log ID)
Top Event Categories	Total Event Count per Severity
Top Event Types	Total Event Count per Software Module
Top Critical Events By Hour	Top Critical Events (by Log ID)
Top Critical Events By Date	Top Critical Events (by Log ID)
Top Warning Events By Hour	Top Warning Events (by Log ID)
Top Warning Events By Date	Top Warning Events (by Log ID)
Top Information Events By Hour	Top Information Events (by Log ID)
Top Information Events By Date	Top Information Events (by Log ID)
Top Emergency Events By Hour	Top Emergency Events (by Log ID)
Top Emergency Events By Date	Top Emergency Events (by Log ID)
Top Alert Events By Hour	Top Alert Events (by Log ID)
Top Alert Events By Date	Top Alert Events (by Log ID)
Top Error Events By Hour	Top Error Events (by Log ID)

Table 23: Event Activity reports

Top Error Events By Date	Top Error Events (by Log ID)
Top Notification Events By Hour	Top Notification Events (by Log ID)
Top Notification Events By Date	Top Notification Events (by Log ID)
Top Events for each Device	Top Events per Device (by Log ID)
Top Event Categories for each Device	Top Event Severities per Device
Top Events by Hour of Day	Top Events (by Log ID)
Top Event Categories by Hour of Day	Total Event Count per Severity
Top Events By Date	Top Events (by Log ID)
Top Event Categories by Date	Top Event Count per Severity
Top Event Types for each Device	Top Software Module Events per Device

The report, Top Event Categories by Status, was removed.

P2P Activity

The following table explains what P2P Activity reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 24: P2P Activity reports

MR6 reports	MR7 reports
P2P Activity by Protocol	Total Events per P2P Protocol
P2P Activity by Action and Date	Total Pass/Block Events (All Protocols)
P2P Activity by Action and Month	Total Pass/Block Events (All Protocols)
P2P Activity by Action and Day of Week	Total Pass/Block Events (All Protocols)
P2P Activity by Action and Hour of Day	Total Pass/Block Events (All Protocols)
Top Allowed P2P Local Peers by Date	Top Allowed P2P Local Peers
Top Allowed P2P Local Peers by Month	Top Allowed P2P Local Peers
Top Blocked P2P Local Peers by Date	Top Blocked P2P Local Peers
Top Blocked P2P Local Peers by Month	Top Blocked P2P Local Peers
Top Allowed P2P Remote Peers by Date	Top Allowed P2P Remote Peers
Top Allowed P2P Remote Peers by Month	Top Allowed P2P Remote Peers
Top Blocked P2P Remote Peers by Date	Top Blocked P2P Remote Peers
Top Blocked P2P Remote Peers by Month	Top Blocked P2P Remote Peers
Top Allowed BitTorrent Local Peers by Date	Top Allowed BitTorrent Local Peers
Top Allowed BitTorrent Local Peers by Month	Top Allowed BitTorrent Local Peers

Table 24: P2P Activity reports

Top Blocked BitTorrent Local Peers by Date	Top Blocked BitTorrent Local Peers
Top Blocked BitTorrent Local Peers by Month	Top Blocked BitTorrent Local Peers
Top Allowed eDonkey Local Peers by Date	Top Allowed eDonkey Local Peers
Top Allowed eDonkey Local Peers by Month	Top Allowed eDonkey Local Peers
Top Blocked eDonkey Local Peers by Date	Top Blocked eDonkey Local Peers
Top Blocked eDonkey Local Peers by Month	Top Blocked eDonkey Local Peers
Top Allowed Gnutella Local Peers by Date	Top Allowed Gnutella Local Peers
Top Allowed Gnutella Local Peers by Month	Top Allowed Gnutella Local Peers
Top Blocked Gnutella Local Peers by Date	Top Blocked Gnutella Local Peers
Top Blocked Gnutella Local Peers by Month	Top Blocked Gnutella Local Peers
Top Allowed KaZaa Local Peers by Date	Top Allowed KaZaa Local Peers
Top Allowed KaZaa Local Peers by Month	Top Allowed KaZaa Local Peers
Top Blocked KaZaa Local Peers by Date	Top Blocked KaZaa Local Peers
Top Blocked KaZaa Local Peers by Month	Top Blocked KaZaa Local Peers
Top Allowed Skype Local Peers by Date	Top Allowed Skype Local Peers
Top Allowed Skype Local Peers by Month	Top Allowed Skype Local Peers
Top Blocked Skype Local Peers by Date	Top Blocked Skype Local Peers
Top Blocked Skype Local Peers by month	Top Blocked Skype Local Peers
Top Allowed WinNY Local Peers by Date	Top Allowed WinNY Local Peers
Top Allowed WinNY Local Peers by Month	Top Allowed WinNY Local Peers
Top Blocked WinNY Local Peers by Date	Top Blocked WinNY Local Peers
Top Blocked WinNY Local Peers by Month	Top Blocked WinNY Local Peers

Audit Activity

The following reports for Audit Activity are unchanged but were moved to a new category in FortiAnalyzer 3.0 MR7.

- System Administration Summary – is now in the Event Activity category
- System Administration Details – is now in the Event Activity category

Summary Reports

The following table explains what Summary reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7, including the category, if applicable, of where the re-named FortiAnalyzer 3.0 MR6 reports were moved to.

Table 25: Summary reports

MR6 reports	MR7 reports	Category that reports were moved to in MR7 (if applicable)
Top Bandwidth Consumers by Source	Top Sources by Volume	Network Analysis
Top Bandwidth Consumption	Traffic Volume per Device	Network Analysis
Top Bandwidth Consumers by Destination	Top Viruses	AntiVirus Activity
Total Viruses Detected	Top Virus Sources	AntiVirus Activity
Top Viruses by Name	Top Virus Destinations	AntiVirus Activity
Top Viruses by Source	Top Devices by Number of Attack Detection	Intrusion Activity
Top Viruses by Destination	Top Attacks	Intrusion Activity
Total IPS Events Detected	Top Destinations by Volume	Network Analysis
Total IPS by Attack ID	Top Devices by Antivirus Violations	AntiVirus Activity
Total IPS by Source	Top Attack Sources	Intrusion Activity
Total IPS by Destination	Top Attack Destinations	Intrusion Activity
Total Spam Activity	Total Spam per Device (by Email Count)	AntiSpam Activity
Bandwidth Consumed by Spam	Total Spam per Device (by Email Size)	AntiSpam Activity
Total Web Filter Activity	Total Hits per Device	WebFilter Activity
Top Web Categories	Top Requested Categories	WebFilter Activity
Top Clients Filtered	Top Blocked Web User	WebFilter Activity
Top Servers Filtered	Top Blocked Web Sites	WebFilter Activity
Total Content Archived	Volume of Filtered Content per Device	Content Activity
Top Archived Content Type	Volume of Filtered Content per Application	Content Activity
Top Archived Sources	Volume of Filtered Content per Source	Content Activity
Total Events Triggered	Total Event Count per Device	Event Activity
Total Events Triggered by Category	Total Event Count per Severity	Event Activity
Protocol Distribution	Top Services by Volume	Network Analysis
Total Events Triggered By Type	Total Event Count per Software Module	Event Activity

The following reports remain unchanged but are moved to a new category in FortiAnalyzer 3.0 MR7:

- Top Spam Destinations is now found in AntiSpam Activity
- Top Spam Sources is now found in the AntiSpam Activity

Forensic Reports

The following forensic reports explain what was changed for FortiAnalyzer 3.0 MR7. These reports are now merged within the other report categories.

Audit

The following table explains what Audit Forensic reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 26: Audit Forensic reports

MR6 reports	MR7 reports	Category that reports were moved to in MR7 (if applicable)
Sites by Blocked Categories	All Blocked Web Sites per Category	AntiSpam Activity
Sites by Permitted Categories	All Allowed Web Sites per Category	AntiSpam Activity
Sites by Access Time	All Requested Web Sites by Time Period	AntiSpam Activity

Detailed

The following table explains what Detailed Forensic reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 27: Detailed Forensic reports

MR6 reports	MR7 reports	Category that reports were moved to in MR7 (if applicable)
Top Client Attempts to Blocked Sites	Top Web Sites for Most Blocked Users	WebFilter Activity
Top Client Attempts to permitted sites by category	Top Allowed Categories for Most Active Users	WebFilter Activity
Top Clients Attempt to blocked sites by category	Top Blocked Categories for Most Active Blocked Users	WebFilter Activity
WebFilter Events by Top destinations and status	Top Web Sites with Status Breakdown (allowed/blocked/etc)	WebFilter Activity
WebFilter Events by timeslice and Destination	Top Requested Web Domains	WebFilter Activity (with time-scale set to by-date)
WebFilter Events by timeslice and URL	Top Requested Web Pages	WebFilter Activity (with time-scale set to by-date)

The report, Top Client Requests to Permitted Sites, was removed.

Summary

The following table explains what Summary Forensic reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7, including the category, if applicable, of where the re-named FortiAnalyzer 3.0 MR6 reports were moved to.

Table 28: Detailed Forensic reports

MR6 reports	MR7 reports	Category that reports were moved to in MR7 (if applicable)
Accessed Categories by Hits	Top Allowed Web Risk Groups	WebFilter Activity
Blocked Categories by Hits	Top Blocked Web Risk Group	WebFilter Activity
Accessed Sub-categories	Top Allowed Sub-Categories	WebFilter Activity (with time-scale set to by-date)
Blocked Sub-categories by Hits	Top Blocked Sub-Categories	WebFilter Activity
Permitted Activity by timeslice	Allowed Web Activity over Time Period	WebFilter Activity
Blocked Activity by timeslice	Blocked Web Activity over Time Period	WebFilter Activity (with time-scale set to by-date)
WebFilter Events by timeslice and status	Total Hits per Status (allowed/blocked/etc)	WebFilter Activity (with time-scale set to by-date)
All Risks	Top Requested Web Risk Group	WebFilter Activity
Blocked Risks	Top Blocked Web Risk Groups	WebFilter Activity
Mail Activities	Spam Activity by Time Period	AntiSpam Activity (with time-scale set to by-date)
Outgoing Mail activity by timeslice	Outgoing Mail Activity by Time Period (SMTP)	Mail Activity (with time-scale set to by-date)
Incoming Mail activity by timeslice	Incoming Mail Activity by Time Period (POP3/IMAP)	Mail Activity (with time-scale set to by-date)

The report, Estimated Browse Time, remains unchanged but is moved to the WebFilter Activity category with the time-scale set to by-date.

FortiMail Reports

The following tables explain what FortiMail reports changed in FortiAnalyzer 3.0 MR7.

Mail High Level

The following table explains what Mail High Level reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 29: Mail High Level reports

MR6 reports	MR7 reports
Top Client IP by Date	Top Client IP

Table 29: Mail High Level reports

Top Client IP by Hour of Day	Top Client IP
Top Client IP by Day of Week	Top Client IP
Top Client IP by Day of Month	Top Client IP
Top Client IP by Week of Year	Top Client IP
Top Client IP by Month	Top Client IP
Top Local User by Date	Top Local User
Top Local User by Hour of Day	Top Local User
Top Local User by Day of Week	Top Local User
Top Local User by Day of Month	Top Local User
Top Local User by Week of Year	Top Local User
Top Local User by Month	Top Local User
Top Remote Address by Date	Top Remote Address
Top Remote Address by Hour of Day	Top Remote Address
Top Remote Address by Day of Week	Top Remote Address
Top Remote Address by Day of Month	Top Remote Address
Top Remote Address by Week of Year	Top Remote Address
Top Remote Address by Month	Top Remote Address
Spam Filter by Date	Spam Filter
Spam Filter by Hour of Day	Spam Filter
Spam Filter by Day of Week	Spam Filter
Spam Filter by Day of Month	Spam Filter
Spam Filter by Week of Year	Spam Filter
Spam Filter by Month	Spam Filter
Action by Date	Disposition Action
Action by Hour of Day	Disposition Action
Action by Day of Week	Disposition Action
Action by Day of Month	Disposition Action
Action by Week of Year	Disposition Action
Action by Month	Disposition Action
Top Virus by Date	Top Virus
Top Virus by Hour of Day	Top Virus
Top Virus by Day of Week	Top Virus
Top Virus by Day of Month	Top Virus
Top Virus by Week of Year	Top Virus
Top Virus by Month	Top Virus
Virus by Date	Top Virus
Virus by Hour of Day	Top Virus
Virus by Day of Week	Top Virus
Virus by Day of Month	Top Virus
Virus by Week of Year	Top Virus

Table 29: Mail High Level reports

Virus by Month	Top Virus
System User by Date	System User
System User by Hour of Day	System User
System User by Day of Week	System User
System User by Day of Month	System User
System User by Week of Year	System User
System User by Month	System User
Top Client MSISDN by Date	Top Client MSISDN
Top Client MSISDN by Hour of Day	Top Client MSISDN
Top Client MSISDN by Day of Week	Top Client MSISDN
Top Client MSISDN by Day of Month	Top Client MSISDN
Top Client MSISDN by Week of Year	Top Client MSISDN
Top Client MSISDN by Month	Top Client MSISDN

Mail Sender

The following table explains what Mail Sender reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 30: Mail Sender reports

MR6 reports	MR7 reports
Top Sender by Date	Top Sender
Top Sender by Hour of Day	Top Sender
Top Sender by Day of Week	Top Sender
Top Sender by Day of Month	Top Sender
Top Sender by Week of Year	Top Sender
Top Sender by Month	Top Sender
Top Sender IP by Date	Top Sender IP
Top Sender IP by Hour of Day	Top Sender IP
Top Sender IP by Day of Week	Top Sender IP
Top Sender IP by Day of Month	Top Sender IP
Top Sender IP by Week of Year	Top Sender IP
Top Sender IP by Month	Top Sender IP
Top Local Sender by Date	Top Local Sender
Top Local Sender by Hour of Day	Top Local Sender
Top Local Sender by Day of Week	Top Local Sender
Top Local Sender by Day of Month	Top Local Sender
Top Local Sender by Week of Year	Top Local Sender
Top Local Sender by Month	Top Local Sender
Top Remote Sender by Date	Top Remote Sender
Top Remote Sender by Hour of Day	Top Remote Sender
Top Remote Sender by Day of Week	Top Remote Sender
Top Remote Sender by Day of Month	Top Remote Sender

Table 30: Mail Sender reports

Top Remote Sender by Week of Year	Top Remote Sender
Top Remote Sender by Month	Top Remote Sender
Top Sender MSISDN by Date	Top Sender MSISDN
Top Sender MSISDN by Hour of Day	Top Sender MSISDN
Top Sender MSISDN by Day of Week	Top Sender MSISDN
Top Sender MSISDN by Day of Month	Top Sender MSISDN
Top Sender MSISDN by Week of Year	Top Sender MSISDN
Top Sender MSISDN by Month	Top Sender MSISDN

Mail Recipient Activity

The following table explains what Mail Recipient Activity reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 31: Mail Recipient Activity reports

MR6 reports	MR7 reports
Top Recipient by Date	Top Recipient
Top Recipient by Hour of Day	Top Recipient
Top Recipient by Day of Week	Top Recipient
Top Recipient by Day of Month	Top Recipient
Top Recipient by Week of Year	Top Recipient
Top Recipient by Month	Top Recipient
Top Local Recipient by Date	Top Local Recipient
Top Local Recipient by Hour of Day	Top Local Recipient
Top Local Recipient by Day of Week	Top Local Recipient
Top Local Recipient by Day of Month	Top Local Recipient
Top Local Recipient by Week of Year	Top Local Recipient
Top Local Recipient by Month	Top Local Recipient
Top Remote Recipient by Date	Top Remote Recipient
Top Remote Recipient by Hour of Day	Top Remote Recipient
Top Remote Recipient by Day of Week	Top Remote Recipient
Top Remote Recipient by Day of Month	Top Remote Recipient
Top Remote Recipient by Week of Year	Top Remote Recipient
Top Remote Recipient by Month	Top Remote Recipient

Mail Destination IP

The following table explains what Mail Destination IP reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7. All Mail Destination IP reports were moved to the Mail Activity category.

Table 32: Mail Destination IP reports

MR6 reports	MR7 reports
Top Mail Destination IP by Date	Top Mail Destination IP
Top Mail Destination IP by Hour of Day	Top Mail Destination IP
Top Mail Destination IP by Day of Week	Top Mail Destination IP
Top Mail Destination IP by Day of Month	Top Mail Destination IP
Top Mail Destination IP by Week of Year	Top Mail Destination IP
Top Mail Destination IP by Month	Top Mail Destination IP

Spam Sender

The following table explains what Spam Sender reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 33: Spam Sender reports

MR6 reports	MR7 reports
Top Spam Sender by Date	Top Spam Sender
Top Spam Sender by Hour of Day	Top Spam Sender
Top Spam Sender by Day of Week	Top Spam Sender
Top Spam Sender by Day of Month	Top Spam Sender
Top Spam Sender by Week of Year	Top Spam Sender
Top Spam Sender by Month	Top Spam Sender
Top Spam Domain by Date	Top Spam Domain
Top Spam Domain by Hour of Day	Top Spam Domain
Top Spam Domain by Day of Week	Top Spam Domain
Top Spam Domain by Day of Month	Top Spam Domain
Top Spam Domain by Week of Year	Top Spam Domain
Top Spam Domain by Month	Top Spam Domain
Top Spam IP by Date	Top Spam IP
Top Spam IP by Hour of Day	Top Spam IP
Top Spam IP by Day of Week	Top Spam IP
Top Spam IP by Day of Month	Top Spam IP
Top Spam IP by Week of Year	Top Spam IP
Top Spam IP by Month	Top Spam IP
Top Local Spam Sender by Date	Top Local Spam Sender
Top Local Spam Sender by Hour of Day	Top Local Spam Sender
Top Local Spam Sender by Day of Week	Top Local Spam Sender
Top Local Spam Sender by Day of Month	Top Local Spam Sender
Top Local Spam Sender by Week of Year	Top Local Spam Sender

Table 33: Spam Sender reports

Top Local Spam Sender by Month	Top Local Spam Sender
Top Local Spam Domain by Date	Top Local Spam Domain
Top Local Spam Domain by Hour of Day	Top Local Spam Domain
Top Local Spam Domain by Day of Week	Top Local Spam Domain
Top Local Spam Domain by Day of Month	Top Local Spam Domain
Top Local Spam Domain by Week of Year	Top Local Spam Domain
Top Local Spam Domain by Month	Top Local Spam Domain
Top remote Spam Sender by Date	Top Remote Spam Sender
Top Remote Spam Sender by Hour of Day	Top Remote Spam Sender
Top Remote Spam Sender by Day of Week	Top Remote Spam Sender
Top Remote Spam Sender by Day of Month	Top Remote Spam Sender
Top Remote Spam Sender by Week of Year	Top Remote Spam Sender
Top Remote Spam Sender by Month	Top Remote Spam Sender
Top Remote Spam Domain by Date	Top Remote Spam Domain
Top Remote Spam Domain by Hour of Day	Top Remote Spam Domain
Top Remote Spam Domain by Day of Week	Top Remote Spam Domain
Top Remote Spam Domain by Day of Month	Top Remote Spam Domain
Top Remote Spam Domain by Week of Year	Top Remote Spam Domain
Top Remote Spam Domain by Month	Top Remote Spam Domain
Top Spam MSISDN by Date	Top Spam MSISDN
Top Spam MSISDN by Hour of Day	Top Spam MSISDN
Top Spam MSISDN by Day of Week	Top Spam MSISDN
Top Spam MSISDN by Day of Month	Top Spam MSISDN
Top Spam MSISDN by Week of Year	Top Spam MSISDN
Top Spam MSISDN by Month	Top Spam MSISDN

Spam Recipient

The following table explains what Spam Recipient reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 34: Spam Recipient reports

MR6 reports	MR7 reports
Top Spam Recipient by Date	Top Spam Recipient
Top Spam Recipient by Hour of Day	Top Spam Recipient
Top Spam Recipient by Day of Week	Top Spam Recipient

Table 34: Spam Recipient reports

Top Spam Recipient by Day of Month	Top Spam Recipient
Top Spam Recipient by Week of Year	Top Spam Recipient
Top Spam Recipient by Month	Top Spam Recipient
Top Local Spam Recipient by Date	Top Local Spam Recipient
Top Local Spam Recipient by Hour of Day	Top Local Spam Recipient
Top Local Spam Recipient by Day of Week	Top Local Spam Recipient
Top Local Spam Recipient by Day of Month	Top Local Spam Recipient
Top Local Spam Recipient by Week of Year	Top Local Spam Recipient
Top Local Spam Recipient by Month	Top Local Spam Recipient
Top Remote Spam Recipient by Date	Top Remote Spam Recipient
Top Remote Spam Recipient by Hour of Day	Top Remote Spam Recipient
Top Remote Spam Recipient by Day of Week	Top Remote Spam Recipient
Top Remote Spam Recipient by Day of Month	Top Remote Spam Recipient
Top Remote Spam Recipient by Week of Year	Top Remote Spam Recipient
Top Remote Spam Recipient by Month	Top Remote Spam Recipient

Spam Destination IP

The following table explains what Spam Destination IP reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 35: Spam Destination IP reports

MR6 reports	MR7 reports
Top Spam Destination IP by Date	Top Spam Destination IP
Top Spam Destination IP by Hour of Day	Top Spam Destination IP
Top Spam Designating IP by Day of Week	Top Spam Destination IP
Top Spam Destination IP by Day of Month	Top Spam Destination IP
Top Spam Destination IP by Week of Year	Top Spam Destination IP
Top Spam Destination IP by Month	Top Spam Destination IP

Virus Sender

The following table explains what Virus Sender reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 36: Virus Sender reports

MR6 reports	MR7 reports
Top Virus Sender by Date	Top Virus Sender
Top Virus Sender by Hour of Day	Top Virus Sender
Top Virus Sender by Day of Week	Top Virus Sender
Top Virus Sender by Day of Month	Top Virus Sender
Top Virus Sender by Week of Year	Top Virus Sender
Top Virus Sender by Month	Top Virus Sender
Top Virus Domain by Date	Top Virus Domain
Top Virus Domain by Hour of Day	Top Virus Domain
Top Virus Domain by Day of Week	Top Virus Domain
Top Virus Domain by Day of Month	Top Virus Domain
Top Virus Domain by Week of Year	Top Virus Domain
Top Virus Domain by Month	Top Virus Domain
Top Virus IP by Date	Top Virus IP
Top Virus IP by Hour of Day	Top Virus IP
Top Virus IP by Day of Week	Top Virus IP
Top Virus IP by Day of Month	Top Virus IP
Top Virus IP by Week of Year	Top Virus IP
Top Virus IP by Month	Top Virus IP
Top Local Virus Sender by Date	Top Local Virus Sender
Top Local Virus Sender by Hour of Day	Top Local Virus Sender
Top Local Virus Sender by Day of Week	Top Local Virus Sender
Top Local Virus Sender by Day of Month	Top Local Virus Sender
Top Local Virus Sender by Week of Year	Top Local Virus Sender
Top Local Virus Sender by Month	Top Local Virus Sender
Top Local Virus Domain by Date	Top Local Virus Domain
Top Local Virus Domain by Hour of Day	Top Local Virus Domain
Top Local Virus Domain by Day of Week	Top Local Virus Domain
Top Local Virus Domain by Day of Month	Top Local Virus Domain
Top Local Virus Domain by Week of Year	Top Local Virus Domain
Top Local Virus Domain by Month	Top Local Virus Domain
Top Remote Virus Sender by Date	Top Remote Virus Sender
Top Remote Virus Sender by Hour of Day	Top Remote Virus Sender
Top Remote Virus Sender by Day of Week	Top Remote Virus Sender
Top Remote Virus Sender by Day of Month	Top Remote Virus Sender

Table 36: Virus Sender reports

Top Remote Virus Sender by Week of Year	Top Remote Virus Sender
Top Remote Virus Sender by Month	Top Remote Virus Sender
Top Remote Virus Domain by Date	Top Remote Virus Domain
Top Remote Virus Domain by Hour of Day	Top Remote Virus Domain
Top Remote Virus Domain by Day of Week	Top Remote Virus Domain
Top Remote Virus Domain by Day of Month	Top Remote Virus Domain
Top Remote Virus Domain by Week of Year	Top Remote Virus Domain
Top Remote Virus Domain by Month	Top Remote Virus Domain
Top Virus MSISDN by Date	Top Virus MSISDN
Top Virus MSISDN by Hour of Day	Top Virus MSISDN
Top Virus MSISDN by Day of Week	Top Virus MSISDN
Top Virus MSISDN by Day of Month	Top Virus MSISDN
Top Virus MSISDN by Week of Year	Top Virus MSISDN
Top Virus MSISDN by Month	Top Virus MSISDN

Virus Recipient

The following table explains what Virus Recipient reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 37: Virus Recipient reports

MR6 reports	MR7 reports
Top Virus Recipient by Date	Top Virus Recipient
Top Virus Recipient by Hour of Day	Top Virus Recipient
Top Virus Recipient by Day of Week	Top Virus Recipient
Top Virus Recipient by Day of Month	Top Virus Recipient
Top Virus Recipient by Week of Year	Top Virus Recipient
Top Virus Recipient by Month	Top Virus Recipient
Top Local Virus Recipient by Date	Top Local Virus Recipient
Top Local Virus Recipient by Hour of Day	Top Local Virus Recipient
Top Local Virus Recipient by Day of Week	Top Local Virus Recipient
Top Local Virus Recipient by Day of Month	Top Local Virus Recipient
Top Local Virus Recipient by Week of Year	Top Local Virus Recipient
Top Local Virus Recipient by Month	Top Local Virus Recipient
Top Remote Virus Recipient by Date	Top Remote Virus Recipient
Top Remote Virus Recipient by Hour of Day	Top Remote Virus Recipient
Top Remote Virus Recipient by Day of Week	Top Remote Virus Recipient

Table 37: Virus Recipient reports

Top Remote Virus Recipient by Day of Month	Top Remote Virus Recipient
Top Remote Virus Recipient by Week of Year	Top Remote Virus Recipient
Top Remote Virus Recipient by Month	Top Remote Virus Recipient

Virus Destination IP

The following table explains what Virus Destination IP reports have changed and what they were changed to in FortiAnalyzer 3.0 MR7.

Table 38: Virus Destination IP reports

MR6 reports	MR7 reports
Top Virus Destination IP by Date	Top Virus Destination IP
Top Virus Destination IP by Hour of Day	Top Virus Destination IP
Top Virus Destination IP by Day of Week	Top Virus Destination IP
Top Virus Destination IP by Day of Month	Top Virus Destination IP
Top Virus Destination IP by Week of Year	Top Virus Destination IP
Top Virus Destination IP by Month	Top Virus Destination IP

FortiClient Reports

The following FortiClient reports remain unchanged after upgrading to FortiAnalyzer 3.0 MR7.

FortiClient Antivirus Activity

- Top Viruses
- Top Files

FortiClient Network Activity

- Top Denied Sources
- Top Denied Destinations

FortiClient WebFilter Activity

- Top Blocked Web Sites
- Top Visited Web Sites
- Top Blocked Web Sites by User
- Top Visited Web Sites by User

FortiClient Antispam Activity

- Top Blocked Mail Senders
- Top Blocked Mail Receivers

Index

A

- access
 - administrative ports 46
 - profile, administrator 48, 50
- access privileges 19
- accounts
 - administrator 48
 - share users 53
- Active Directory. *See* LDAP
- ActiveX. *See* web filtering
- adding tabs 27
- admin
 - access 46
 - authentication 51
 - disconnect 52
 - idle timeout 52
 - password 49, 50
 - privileges 50
- administrative access 45
- Administrative Domains (ADOM) 19, 21, 22, 23, 48, 52, 74
 - administrators 24
 - root 23
- AGGREGATOR 46
 - See also* SSH
- alert 133
 - acknowledge 34
 - console messages 34
 - display on dashboard 34
 - events 57, 58, 133
 - mail server 135
 - sending 134
 - SNMP traps 136
 - Syslog server 140
 - threshold 134
 - triggers 133, 134
- alias. *See* IP alias
- allocate disk space. *See* disk space
- Apple Mac OS X 157, 161
- array. *See* RAID
- audit 157
- authentication 51
- Automatic Discovery 47, 85

B

- backing up configuration
 - using the CLI 170
 - using web-based manager 170
- backing up log files 170
- backup 69
- blocked devices 77, 79, 86
- Boolean operator 99, 111, 150
- browse

- log 93
 - network analyzer 144
 - sniffer 144
- buffer overflow 157

C

- character set 126, 127
- CLI 10, 46
 - enable Network Analyzer 141, 142
 - set share permissions 56
- cluster. *See* high availability (HA)
- column view
 - content logs 109
 - logs 97
 - network analyzer logs 148
- common name (CN) 69
 - See also* LDAP
- compression. *See* gzip
- configuration file
 - backup 69
 - install by FortiManager unit 46
 - password 70
- connection
 - attempt handling 73, 74, 79
 - sessions 35
 - to sniff network traffic 141
- content archive 107
 - filter 110
 - from device 73
- content logs
 - column view 109
 - formatted view 109
- CPU usage 31, 32

D

- dashboard
 - intrusion activity 38
 - log receive monitor 37
 - raid monitor 28
 - tabs 27
 - top email traffic 41
 - top ftp traffic 40
 - top im/p2p traffic 42
 - top traffic 43
 - top web traffic 44
 - virus activity 39
- DC (duplicate count) 132
- default
 - route 47
 - share permissions 55, 56
- delete after upload
 - logs 105
 - network analyzer log 155

- deleting tabs 27
 - denial of service (DoS) 158
 - device
 - add 80
 - alerts 133
 - blocked 77, 79, 86
 - group 88
 - HA *See also* high availability (HA) 76, 82
 - license 31, 76
 - maximum allowed 76
 - permissions 73, 74, 82, 83
 - registration and reports 79, 91, 114, 131
 - unregistered 77, 79, 91, 114
 - secure connection. *See* secure connection
 - Device ID 75, 81
 - Device Name 75
 - See also* Local ID
 - direction, traffic 84
 - disk space
 - allocated to device 75, 82
 - allocated to Network Analyzer 154
 - See also* hard disk
 - distinguished name (DN) 69
 - See also* LDAP
 - DMZ 84
 - DNS 47
 - double-byte encoding 126, 127
 - downgrading to FortiLog 1.6 177
 - download
 - configuration file 69
 - logs 96, 103, 153
 - network analyzer logs 147
 - search results 103, 153
 - dynamic NAT 158
- ## E
- editing charts, report profiles 116
 - email
 - alert 134
 - content archive 107
 - subject 165
 - encoding 126, 127
 - encoding, double-byte 126, 127
 - ESP 86
 - event
 - severity threshold 57, 58
 - exploit 162
 - export, NFS 47, 53
- ## F
- factory default configuration 33
 - FDN
 - connecting through a web proxy 71
 - connection 71
 - Fortinet Distribution Network 70, 71, 162
 - FDP
 - Fortinet Discovery Protocol 47, 85
 - icon 45
 - file
 - extension 96, 97, 104, 147, 153, 165, 170
 - format 165
 - permissions 55, 56
 - transfer 107
 - file explorer 167
 - filter
 - content archive 110
 - criteria 99, 110, 150
 - icon 36, 96, 98, 100, 110, 147, 149, 150
 - logs 98
 - network analyzer 149
 - session 36
 - tip 99, 110, 150
 - web 107
 - fingerprinting 166, 167
 - firmware
 - downgrade 30, 69
 - image 69
 - image integrity check 181
 - restore 180
 - upgrade 30, 69
 - upload 69
 - version 29, 70
 - fnTrapFlgEventCount 138
 - font file 126
 - forensic reports in 3.0 MR7 202
 - format file 126
 - format hard disk 33
 - formatted view
 - content logs 109
 - logs 97
 - network analyzer logs 148
 - FortiAnalyzer
 - device load 76
 - MIB 138
 - restore 180
 - FortiClient 76, 88
 - add 80
 - and remote vulnerability scans 158
 - FortiClient reports in 3.0 MR7 212
 - FortiDiscovery. *See* FDP
 - FortiGate 81
 - add 80
 - and remote vulnerability scans 158
 - group 83
 - HA 76
 - interface specifications 84
 - FortiGate reports in 3.0 MR7 185
 - FortiGuard
 - Center 71
 - subscription service 71
 - Web Filtering 107
 - See also* web filtering
 - FortiMail
 - add 80
 - group 83
 - HA 76
 - FortiMail reports in 3.0 MR7 203
 - FortiManager 81
 - add 80
 - group 83
 - remote administration of FortiAnalyzer 46, 81
 - Fortinet Distribution Network *See* FDN

Fortinet MIB 138
 Fortinet Technical Support 11, 138
 FTP
 content archive 107
 upload to 105, 155

G

gateway 47
 gid 54
 Global Configuration 20
 group
 device 83, 88
 share users 54
 group ID (gid) 161
 Group Policy Object Editor 159
 gzip 96, 97, 104, 105, 147, 153, 155, 170

H

halt 33
 hard disk
 controller 64
 format 33
 hot spare 64
 hot swap 64
 replace failed 65
 status 32
 usage 32
 See also RAID
 high availability (HA) 76, 81, 82, 83, 85
 device ID 82, 83
 historical viewer
 log 92
 network analyzer 143
 host name 29
 See also DNS
 hot spare. See hard disk
 hot swap. See hard disk
 HTTP 46
 content archive 107
 See also protocol
 HTTPS 46
 See also protocol

I

idle timeout 52
 IKE 86
 import
 configuration file 69
 IP alias file 61
 log files 95
 indexed log fields 100, 150
 instant message (IM)
 content archive 107
 interface
 administrative access 46
 configuration 45
 status 45
 intrusion activity, dashboard 38
 intrusion prevention system (IPS) 158
 IP address 45, 46

IP alias 35, 60
 importing from file 61
 resolve host names 108
 IPSec VPN tunnel 74, 86
 log 57

K

known device type 79

L

LAN 84
 language
 administrator 52
 report 126
 resource file 126, 128
 LCD panel 52
 LDAP 68
 LI 15
 license information 31
 See also RVS
 line endings 128
 Linux 157, 160
 local exploit 157
 Local ID 75
 See also IPSec VPN tunnel
 locale 52
 localization 126
 log
 aggregation 46, 58, 73
 automatically delete 58
 browse 93
 compression. See gzip
 content. See content archive
 CSV format 96, 170
 forwarding 60, 73
 gzip 96, 97, 104, 105, 147, 153, 170
 historical viewer 92
 level 57, 58
 real-time viewer 91
 roll settings 104
 search 100, 150
 secure tunnel 57, 74, 86
 settings 57
 threshold 58, 60
 to Syslog server 57
 traffic on device interfaces 84
 volume 35
 VPN 74
 log receive monitor, dashboard 37
 logs
 column view 97
 CSV format 97, 104, 147, 153
 delete after upload 105
 download 96, 103, 153
 filter 98
 formatted view 97
 import 95
 indexed fields 100, 150
 raw view 98, 100, 110, 149, 150
 resolve host names 94, 143
 unindexed fields 98, 100, 110, 149, 150

M

- mail server 135
- Main Menu 20
- managing firmware
 - backing up configuration using the CLI 170
 - backing up configuration using web-based manager 170
 - backing up log files 170
 - downgrading to FortiLog 1.6 177
 - downgrading to FortiLog 1.6 using the CLI 178
 - patch releases 169
 - restoring configuration using CLI 180
 - restoring configuration using the CLI 182
 - restoring configuration using web-based manager 182
 - testing firmware before upgrading 172
 - upgrading to FortiAnalyzer 3.0 174
 - upgrading using the CLI 175
 - upgrading using web-based manager 174
 - verifying downgrade to FortiLog 1.6 178
 - verifying upgrade to FortiAnalyzer 3.0 176
- maximum
 - allowed devices 76
- memory status 31
- MIB 138
- Microsoft Windows 157
- mirroring 63
 - See also* RAID
- modules, vulnerability. *See* RVS

N

- NAS 53, 54
- NAT device 71
- NetBIOS 158
- NetBIOS. *See* share
- network
 - attached server (NAS) 53, 54
 - file system (NFS) 53
 - mask 45, 46
 - sniffer 144
 - time protocol 29
- network analyzer
 - browse 144
 - column view 143
 - delete after download 155
 - download logs 147
 - enable 141, 154
 - filter 149
 - gzip 155
 - historical viewer 143
 - real-time viewer 143
 - resolve host names 143, 145
 - roll settings 153
 - upload to 155
- network analyzer logs
 - column view 148
 - formatted view 148
- NFS 53
 - share 47
- NTP 29

O

- OFTP 86
- override server 71
 - See also* FDS
- overwrite older messages 82

P

- password 48, 49
 - configuration file 70
 - log upload 155
 - share user 54
- patch releases 169
- PDF objects 127
- permissions 19, 56
 - admin 48, 50
 - device 74, 83
 - Guest 159
 - incorrect 157
 - share 55, 56
- PIN 52
- PING 46
- port
 - 123 29
 - 22 46, 58
 - 23 46
 - 3000 46
 - 389 68
 - 443 46
 - 514 86
 - 69 180
 - 80 46
 - 8080 46
 - destination 143
 - device 84
 - scan 157, 164
- port address translation (PAT) 158
- port forwarding 158
- port scan 157
- power cycle 33
- power off 33
- pre-shared secret (PSK) 75
- primary unit 82, 83
- privileges, admin. *See also* permissions, admin 50
- profile, report 114
- protocol 73
 - ESP 86
 - FDP 46, 47, 85
 - FTP 105, 155
 - HTTP 46
 - HTTPS 46
 - ICMP (ping) 46
 - ICQ *See* content archive
 - IKE 86
 - LDAP 68
 - NetBIOS 158
 - NetBIOS. *See* share
 - NFS 54
 - NTP 29
 - OFTP 86
 - RADIUS 49
 - SCP 105, 155

- SFTP 105, 155
 - SNMP 73
 - SOAP 46
 - SSH 46, 58, 160
 - telnet 46
 - TFTP 180
 - UDP 47, 85
 - VoIP 107
 - PSK 75
 - See also IPSec VPN tunnel
- ## Q
- quarantine 131
 - duplicate count 132
 - from device 73
 - ticket number 131
 - quota. See disk space
- ## R
- RADIUS 49, 51
 - RAID 62, 64
 - hot swap 64
 - status 32
 - raid monitor, dashboard 28
 - RAM usage 31
 - real-time viewer
 - log 91
 - network analyzer 143
 - reboot 33
 - refresh interval 35
 - remote access ports 46
 - remote administration 46, 73, 81
 - protocols 45, 46
 - renaming tabs 27
 - report
 - browsing reports 130
 - configuring data filter templates 121
 - configuring output templates 123
 - device registration 79, 91, 114
 - language customization 126
 - localization 126
 - profile 114
 - remote vulnerability sscan (RVS) 157
 - report schedules 118
 - vulnerability 166
 - reports
 - editing charts 116
 - reports in 3.0 MR7
 - forensic reports 202
 - FortiClient reports 212
 - FortiGate reports 185
 - FortiMail reports 203
 - reset
 - configuration 30, 33
 - resolve host names 35, 60, 108
 - logs 94, 143
 - network analyzer 143, 145
 - See also IP alias
 - restart 33
 - restore
 - configuration file 69
 - default configuration 33
 - firmware 180
 - the FortiAnalyzer unit 180
 - restoring 2.80MR11 configuration 180
 - restoring configuration 180
 - RFC
 - 1213 138
 - 2665 138
 - roll settings
 - log 104
 - network analyzer 153
 - root (Management Administrative Domain) 23
 - route
 - default 47
 - static 47
 - RVS 157
 - job options 164
 - jobs 162
 - login 164
 - modules 161
 - port range 164
 - report 166
 - update immediately 71, 72
 - update schedule 71, 72
 - update subscriptions 71
 - upgrade file 71
 - version 71
 - See also FDN
 - See also FortiGuard Center
 - Rx. See device permissions 74
- ## S
- scan
 - report 162
 - target 164
 - SCP
 - upload to 105, 155
 - search
 - content archive 107
 - download results 103, 153
 - logs 100
 - Network Analyzer logs 141, 150
 - tips 102, 152
 - user data 107
 - secure connection 57, 74, 86, 131
 - icon 74
 - security policy, Microsoft Windows 159
 - serial number 29
 - See also Device ID
 - session 32, 35
 - sessions 35
 - SFTP
 - upload to 105, 155
 - share
 - group 54
 - NFS 47, 53
 - permissions 55, 56
 - users 53
 - Windows 53, 54
 - shut down 33
 - SMB 53
 - SMTP 135

- sniffer 141, 144
 - See also network analyzer
 - SNMP 73
 - manager 138
 - MIB 138
 - server, test 137
 - traps 136
 - SOAP 46
 - span port 141
 - SSH 46, 160
 - See also protocol
 - stop logging 82
 - string file 126
 - striping 63
 - See also RAID
 - subject 165
 - subnet 47, 85, 102, 152
 - subscription service 71
 - suspicious
 - events 34
 - sync interval 29
 - syntax 127
 - Syslog
 - add 80
 - device 81
 - group 83
 - log to server 57
 - server 140
 - See also log forwarding
 - system settings
 - restore default 33
 - time 29
- ## T
- tabs
 - adding tabs to dashboard 27
 - deleting 27
 - renaming 27
 - TELNET 46
 - See also protocol
 - test
 - device connectivity 86
 - FortiAnalyzer connectivity (PING) 46
 - mail server 136
 - SNMP server 137
 - testing firmware before upgrading 172
 - TFTP server 180
 - threshold
 - alert 134
 - forwarding 60
 - logging 58
 - ticket number 131
 - time
 - NTP server 29
 - settings 29
 - sync interval 29
 - top email traffic, dashboard 41
 - top ftp traffic, dashboard 40
 - top im/p2p traffic, dashboard 42
 - top traffic, dashboard 43
 - top web traffic, dashboard 44
- traffic
 - sessions 32, 35
 - traps
 - SNMP 136
 - trusted host 48, 49
 - tunnel 86
 - Tx. See device permissions 74
- ## U
- uid 54
 - unindexed log fields 98, 100, 110, 149, 150
 - Unix 157, 161
 - unknown device type 79
 - unregistered device 77, 79, 91, 114, 131
 - options 74
 - upgrade
 - firmware 30
 - FortiGuard services 71
 - upgrading
 - 3.0 using the CLI 175
 - 3.0 using web-based manager 174
 - using the web-based manager 174
 - uptime 29
 - user
 - accounts 53
 - group 54
 - of shares 53
- ## V
- verifying
 - upgrade to 3.0 176
 - verifying downgrade to FortiLog 1.6 178
 - virtual domains (VDOM) 19, 76
 - virus
 - See quarantine
 - virus activity, dashboard 39
 - VLAN 83, 84
 - See also virtual domains (VDOM)
 - VoIP 107
 - VPN
 - See also IPSec VPN tunnel
 - vulnerability
 - modules 161
 - report 166
 - scan target 164
 - See also RVS
- ## W
- WAN 84
 - warning 34, 133
 - web
 - filtering 102, 107
 - WEBSERVICES 46, 81
 - what's new for 3.0MR7 13
 - what's new, 3.0 MR7
 - alert email config changes 17
 - CLI tasks, upload queue 15
 - custom fields, log messages 16
 - dashboard enhancements 15

registered device's hard limits 15
report configuration enhancements 16
voip reports 17
Windows AD. See LDAP

Windows shares 53, 54

X

XML. See WEBSERVICES



www.fortinet.com

FORTINET™

www.fortinet.com