



**New features for
FortiAnalyzer 3.0 MR6**

FORTINET™

www.fortinet.com

New features for FortiAnalyzer 3.0 MR6
31 January 2008
02-30006-0441-20080131

© 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

Contents

3.0 MR6 features and changes.....	5
Overview of new features and changes	5
New features and changes	7
FortiAnalyzer unit supported devices increase/decrease.....	7
Co-ordinated Universal Time (UTC).....	7
Software RAID default setting changes	7
Dashboard enhancements	7
SNMP access list	8
Log	8
Log message changes.....	8
Searching logs	9
Importing log files.....	9
Content archive	9
Reports.....	9
Report enhancements	10
Language support for reports	11
Forensic Analysis reports	11
Daylight Saving Time (DST) in reports	12
High Availability (HA)	12

3.0 MR6 features and changes

FortiAnalyzer 3.0 MR6 provides new features, such as an enhanced dashboard and support for FortiManager units in high availability mode, as well as several changes to existing features. Changes to existing features include logs, reports, and log search capabilities.

The following sections contain information specific to FortiAnalyzer 3.0 MR6.

- [Overview of new features and changes](#)
- [New features and changes](#)

Fortinet recommends reading the following documents for any additional information that concerns the new features and changes in FortiAnalyzer 3.0 MR6.

- *FortiAnalyzer Administration Guide*
- *FortiAnalyzer CLI Reference*



Note: See the *Release Notes for FortiAnalyzer 3.0 MR6* to review both the resolved issues and current known issues concerning FortiAnalyzer 3.0 MR6.

It is recommended to back up current configuration before upgrading to FortiAnalyzer 3.0 MR6; this ensures configuration settings can be restored in the event they are not carried forward during the upgrade.

FortiAnalyzer 3.0 MR6 supports the FortiAnalyzer-800B unit.

Overview of new features and changes

New features for FortiAnalyzer 3.0 MR6 are:

- **Maximum number of supported devices** – The maximum number of supported devices for the FortiAnalyzer-4000A and FortiAnalyzer-800 have changed. See [“FortiAnalyzer unit supported devices increase/decrease” on page 7](#) for more information.
- **Co-ordinated Universal Time (UTC)** – The UTC is now the default standard time on the FortiAnalyzer unit. See [“Co-ordinated Universal Time \(UTC\)” on page 7](#) for more information.
- **Software RAID default setting changes** – The default setting for software RAID has changed from 5 to 10 on certain FortiGate units. See [“Software RAID default setting changes” on page 7](#) for more information.
- **Dashboard enhancements** – The Dashboard widgets can now be rearranged in any order you want as well as adding and removing widgets. See [“Dashboard enhancements” on page 7](#) for more information.
- **SNMP Access list** – The FortiAnalyzer unit now accepts SNMP queries from any IP address if the SNMP community is 0.0.0.0. See [“SNMP access list” on page 8](#) for more information.

- **Log message changes** – There are several log message changes for FortiAnalyzer 3.0 MR6. See [“Log message changes” on page 8](#) for more information.
- **Log search enhancements** – The search has been enhanced, with additional filters. See [“Searching logs” on page 9](#) for more information.
- **Importing log files** – When importing log files, devices can be automatically added if the device is not in the list. See [“Importing log files” on page 9](#) for more information.
- **Content Archive search enhancements** – The tab, Search, was added to the Email Archive menu so that you can search for archived emails. See [“Content archive” on page 9](#) for more information.
- **Report enhancements** – Reports have several enhancement, such as Forensic Analysis search. See [“Report enhancements” on page 10](#) for more information.
- **Language support for reports** – You can now customize the language for your reports. See [“Language support for reports” on page 11](#) for more information.
- **Forensic Analysis reports** – Forensic analysis reports are now simplified and merged into the Report menu. See [“Forensic Analysis reports” on page 11](#) for more information.
- **Daylight Saving Time resolved in reports** – The daylight savings time issue is now resolved for all reports. See [“Daylight Saving Time \(DST\) in reports” on page 12](#) for more information.
- **High Availability (HA)**– You can now add FortiManager units that are in a HA cluster to the FortiAnalyzer unit. See [“High Availability \(HA\)” on page 12](#) for more information.

New features and changes

The following descriptions include only menus containing new features, changes to features or both. Procedural information is included where applicable.

FortiAnalyzer unit supported devices increase/decrease

The FortiAnalyzer-800 and FortiAnalyzer-4000A support different maximum number of devices. The FortiAnalyzer-800 now supports 5000 FortiClient installations, an increase from FortiAnalyzer 3.0 MR5. The FortiAnalyzer-4000A now supports only 500 devices, a decrease from FortiAnalyzer 3.0 MR5.

Co-ordinated Universal Time (UTC)

UTC is now the default time on the FortiAnalyzer unit. UTC is an atomic standard and has uniform seconds defined by the International Atomic Time (ATI) with leap seconds announced at irregular intervals to compensate for the Earth's slowing rotation and other discrepancies.

Software RAID default setting changes

The software RAID default setting for FortiAnalyzer-800 and FortiAnalyzer-400 units with software RAID has changed to 10 as the default RAID setting.

If an administrator tries to enable RAID, a warning displays similar to the following:

```
WARNING! If the RAID level is changed, ALL data will be
DELETED! The disk quota of each device might be reduced to
fit within the new RAID! Changing the level may take a
minutes. Continue?
```

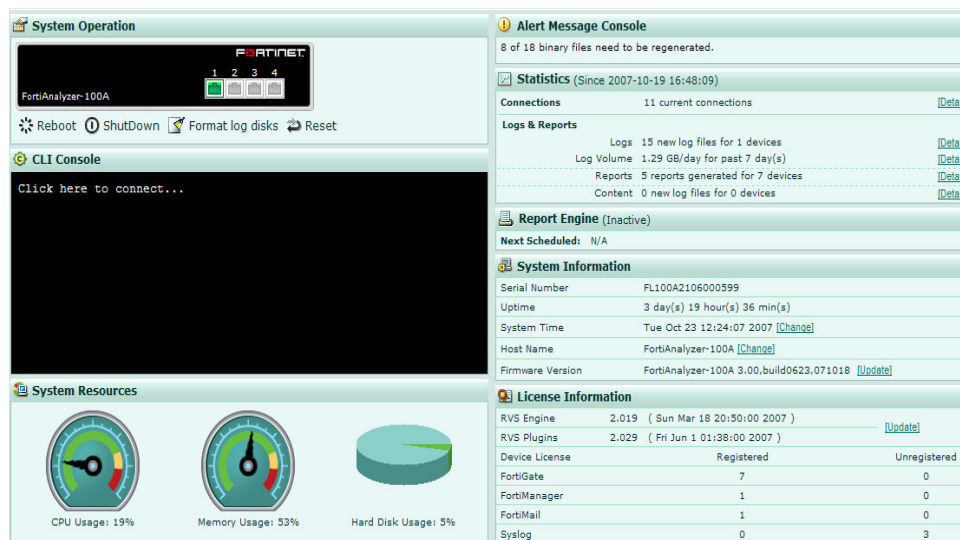
You can restore the default RAID setting back to 10 in the CLI.

Dashboard enhancements

The System menu contains enhancements to the Dashboard in FortiAnalyzer 3.0 MR6.

The Dashboard has been enhanced for better flexibility as well as better viewing system information on the FortiAnalyzer unit. The widgets can be rearranged by using your mouse to drag and drop them anywhere on the Dashboard.

Figure 1: Dashboard enhancements on a FortiAnalyzer-100A



You can also add or remove widgets from the Dashboard by selecting the Edit icon. There are several icons available with each widget that are hidden until you move your mouse over the widget name.

In the License Information widget, FortiGate units and Syslog servers are now separate with each one clearly represented.

SNMP access list

In **Alert > Output > SNMP Access List**, the IP address option, 0.0.0.0, is now available. This IP address enables the FortiAnalyzer unit to accept traps (queries) from any IP address. Alerts are still only sent to a specific IP address, and do not work if the IP address of the SNMP community is set to 0.0.0.0.

Log

The Log menu contains enhancements for importing log files and searching log files. Log message changes also included because they affect FortiAnalyzer 3.0 MR6.

Log message changes

The following are changes to log messages that affect FortiAnalyzer 3.0 MR6:

- Policy ID is included in FortiGate logs to enhance the usability of FortiAnalyzer reporting feature that uses data-filter.
- Log messages now display the banned word in the log message
- File filter and filtype fields are now included in FortiGate log messages
- Session ID (SN) field is now added to FortiGate content archive logs

If logs fail to upload from the FortiAnalyzer unit, for example to an FTP site, the logs are now retrieved when the FTP becomes available again, or during the next upload.

Searching logs

The search method has been enhanced to provide better searching capabilities. Additional filters were added, including log type, log severity, and other log message fields. You can still perform a quick search as well as a full search.

Figure 2: Configuring log search in Log > Search > Log Search

When search results display in **Log > Search > Log Search**, they are displayed as found, not at the end of a search. The More Options section must be expanded to configure search using other filters.



Note: Quick search searches fields that are indexed; this type of search cannot start with a wild card, such as “*”. Full search searches fields that are indexed but also ones that are not indexed, and containing quotes, such as Message; other search terms can be preceded with wilds cards because it is full text search. Full search is usually slower because of this.

Importing log files

When importing log files, the FortiAnalyzer unit can now detect the `device_id` field from within the log file and add that log file to the correct device. If the correct device does not exist, the FortiAnalyzer unit can be configured to prompt you and automatically add the device as well as the log file. For example, the FortiGate-60 unit is not in the list but the log file for the FortiGate-60 is currently being imported; the FortiAnalyzer unit then prompts you to automatically add the FortiGate-60 and import the FortiGate-60 log file.

Content archive

In **Content Archive > Email Archive**, a Search tab is available for searching emails that are archived on the FortiAnalyzer unit. The Search tab provides the following options:

From	The sender's email address.
To	The receiver's email address.
Subject	The subject of the particular email you want to search.
Message Contains	This is the body of the email message, any text that may
Device	Search all FortiGate units or select a specific FortiGate unit to search.
Date Within	The time interval to search in.

Reports

The Report menu now contains support for importing and exporting languages for reports and a new tab, Forensic, in **Report > Browse**. Reports have been enhanced for FortiAnalyzer 3.0 MR6 as well.

Report enhancements

You can no longer delete a report subsection in **Log & Report > Browse**. The Delete icon was removed because of issues with HTML reports.

In **Report > Config**, the Device Audit tab is now called Device Detail.

Previously, report titles displayed only the first subnet; this issue is now resolved, and reports titles now display each subnet separated with an OR.

Previously, a report that was interrupted when an administrator rebooted the system would not re-generate the report. In FortiAnalyzer 3.0 MR6, reports that are generating when an administrator reboots the system, are generated again after the reboot to complete the report.

Report changes fall into these categories:

- new reports – for example, Top Web Users by Web Time
- existing reports that are renamed – for example, Top Web Clients by Browse Time is now Top Web Sources by Browse Time
- labels in existing reports are renamed – for example, the “user” field is now called the “source” field in the Top Sources of Attacks report

Figure 3 shows the report types available for configuring reports.

If log data matching the report scope and criteria does not exist for a report type, or if log index and binary files have not yet been generated for those logs, a message appears in the generated report: “No matching log data for this report.”

Figure 3: Available types of reports in the Device Summary menu






































Language support for reports

FortiAnalyzer 3.0 MR6 now supports multiple language files for Reports that are imported and exported by the administrator. By importing or exporting languages, an administrator can customize what language is used in a report.

Languages are imported or exported from **Report > Config > Language**. In the Language page, you can do one of the following:

Figure 4: Languages as displayed on the Language page in the Report menu

Create New			
Language	Description	Font	Action
English	English	Arial	    
Japanese	Japanese		    
SampleLang	A sample language customization.	Arial	    
Simlish	Simlish	Arial	    
Simplified_Chinese	Simplified Chinese		    
Spanish	Spanish		    
Traditional_Chinese	Traditional Chinese		    

Edit	Select to edit and modify the description of the language file, including changing the type of format, string and font file.
Delete	Select to delete the language file from the FortiAnalyzer unit.
Download Format File	Select to download the format file to the management computer.
Download String File	Select to download the language string file
Download Font File	Select to download the style of font used, for example, Arial.

The text in tables and graphics are translated into the language that is selected. You can select from English, Japanese, Simplified Chinese, Spanish, and Traditional Chinese.

Figure 5: Importing a new report language

Add Report Language

Language:

Description:

Format File:

String File:

Font File: (Optional)

Forensic Analysis reports

The forensic analysis reports that were available in FortiAnalyzer 3.0 MR5 have been simplified and merged into the Report menu. You can browse Forensic reports from **Report > Browse > Forensic**. You can create reports that include Forensic data from **Report > Config > User/Client** and **Report > Config > Device Audit**.

Both User/Client and Device/Audit reports include former forensic report options. User/Client reports can include sub-reports of many types, focusing on different aspects or levels of detail.

Daylight Saving Time (DST) in reports

The DST time period issue in the report scope area of all reports is now resolved. Previously, if DST was enabled, and the time period included a time change due to DST, then the time period would not be completely accurate. This resolved issue is for only those FortiAnalyzer units that use DST.

High Availability (HA)

You can now add FortiManager units that are part of a HA cluster to the device list. They are represented as a single entity, the same as when adding FortiGate units that are part of a HA cluster.

FORTINET™

www.fortinet.com

FORTINET™

www.fortinet.com