FortiAnalyzer v4.0 MR3 Patch Release 8

Release Notes

FortiAnalyzer v4.0 MR3 Patch Release 8 Release Notes

November 28, 2013

05-438-224854-20131128

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2013-11-26	Initial release.
2013-11-28	Added bug ID 196770 to Resolved Issues.

Introduction

This document provides a summary of enhancements, support information, installation instructions, integration, resolved and known issues in FortiAnalyzer v4.0 MR3 Patch Release 8 build 0719.

Supported models

The following models are supported on FortiAnalyzer v4.0 MR3 Patch Release 8.

FortiAnalyzer

FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, and FAZ-4000B.

FortiAnalyzer 800 is no longer supported (EOS) as of October 16, 2012.
FortiAnalyzer 2000 is no longer supported (EOS) as of February 14, 2013.
FortiAnalyzer 4000 is no longer supported (EOS) as of March 1, 2012.
FortiAnalyzer 4000A is no longer supported (EOS) as of June 13, 2013.

FortiAnalyzer VM

FAZ-VM32 and FAZ-VM64.

See http://docs.fortinet.com/fa.html for additional documents on FortiAnalyzer v4.0 MR3.

For more information on Fortinet product life cycle for Fortinet hardware and software, see *Resource Center* > *Product Life Cycle* on the Customer Service & Support site.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer v4.0 MR3 Patch Release 8 build 0719.

TFTP boot process

The TFTP boot process erases all current configuration and replaces it with the factory default settings.

Monitor settings for Web-based Manager access

Fortinet recommends setting your monitor to a screen resolution of 1280x1024. This allows for all the objects in the Web-based Manager to be viewed properly.

Before any upgrade

Save a copy of your FortiAnalyzer unit configuration prior to upgrading. Go to *System* > *Maintenance* > *Backup & Restore,* select the *Backup* button to save the configuration file to your local hard drive.

After any upgrade

If you are using the Web-based Manager, clear the browser cache prior to login on the FortiAnalyzer to ensure the Web-based Manager screens are displayed properly.

To add a secondary log aggregation target

In the CLI command `config system operation`, when the FortiAnalyzer is set as a collector, the following commands were added to support a secondary log aggregation target:

```
set server-ip-2 <ip_address>
set password-2 <password>
```

In the CLI command `config log aggregation`, the following commands were added:

```
set server_ip_2 <ip_address>
set password_2 <password>
set aggregation_time_2 <hour>
```

Stackable license model for FortiAnalyzer VM

Customers who purchase a version 5.0 FortiAnalyzer VM license can now apply this license to their existing version 4.0 MR3 FortiAnalyzer VM environment. When applying the v5.0 license to v4.0 MR3 you are required to use FortiAnalyzer v4.0 MR3 Patch Release 8.

Upgrade Information

Upgrading from FortiAnalyzer v4.0 MR3 Patch Release 5 or later

FortiAnalyzer v4.0 MR3 Patch Release 8 build 0719 officially supports upgrade from the FortiAnalyzer v4.0 MR3 Patch Release 5 build 0680 or later.

Please review the Special Notices, Product Integration and Support, and Known Issues chapters prior to upgrading. For more information on upgrading your FortiAnalyzer device, see the *FortiAnalyzer v4.0 MR3 Patch Release 7 Administration Guide* at http://docs.fortinet.com.

Upgrading from FortiAnalyzer v4.0 MR2 Patch Release 6

FortiAnalyzer v4.0 MR3 Patch Release 8 build 0719 officially supports upgrade from the FortiAnalyzer v4.0 MR2 Patch Release 6 build 0240.

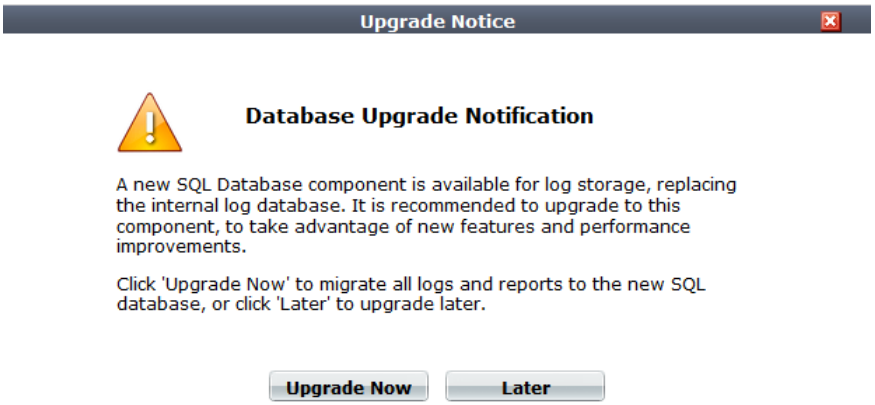
Database upgrade notification

FortiAnalyzer v4.0 MR3 Patch Release 8 contains significant performance enhancements for SQL logging and reporting. To accommodate this change, it was necessary to improve the schema in how logs are stored in the database. Please follow read the instructions below before upgrading the FortiAnalyzer firmware.

If local or remote SQL database is disabled before upgrading to FortiAnalyzer v4.0 MR3 Patch Release 8, complete the following step:

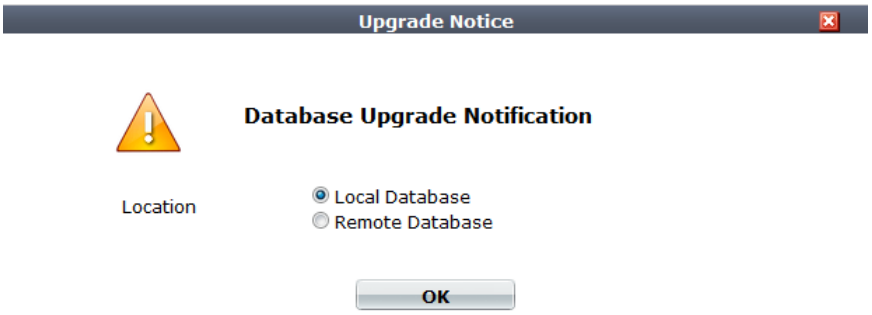
1. After the firmware upgrade is complete and the system has rebooted, you will see a reminder message after logging in through the Web-based Manager. If you select *Later,* the FortiAnalyzer device will continue to use indexes for its log storage and reporting.

Figure 1: Database upgrade notification



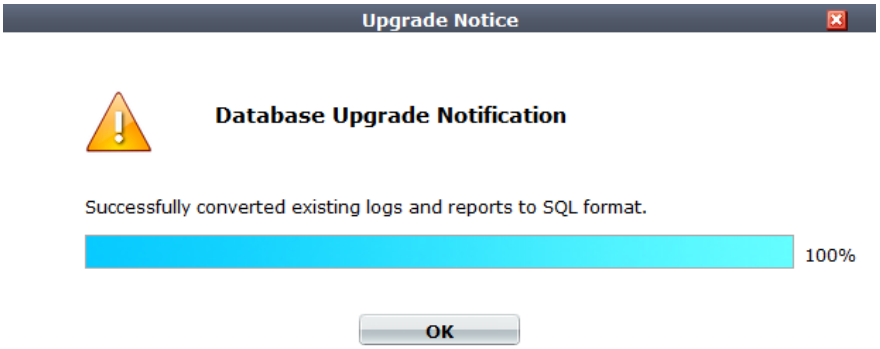
2. If *Upgrade Now* is selected, you must choose to use either a local SQL database or a remote SQL database.

Figure 2: Location selection



3. After the conversion process is finished, all existing logs are transferred to the SQL database.

Figure 3: Successful conversion notification



If local or remote SQL database is enable before upgrading to FortiAnalyzer v4.0 MR3 Patch Release 8, complete the following steps:

1. After the firmware upgrade is complete and the system has rebooted, disable the SQL database in the Web-based Manager under *System* > *Config* > *SQL Database*.
2. If you are using the local SQL database, delete the local database using the CLI command `execute sql-local remove-db`. Your previous log messages are recoverable in Step 4 and 5 below.
3. If you are using a remote SQL database, remove the database for the FortiAnalyzer device at the remote MySQL server side. Your previous log messages still are recoverable in Step 4 and 5 below.
4. Run the CLI command `execute reset-sqllog-transfer`.
5. From Web-based Manger, browse to *System* > *Config* > *SQL Database*, select a time from when you want to begin recovering the database, and enable the local or remote SQL database. All logs starting from this time will be recovered.

Downgrade information

Downgrading from FortiAnalyzer v4.0 MR3 Patch Release 8 build 0719 to previous releases is not supported.

Product Integration and Support

Web browser support

FortiAnalyzer v4.0 MR3 Patch Release 8 supports the following web browsers:

- Microsoft Internet Explorer versions 9 and 10
- Mozilla Firefox versions 24 and 25
- Google Chrome version 31

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiAnalyzer v4.0 MR3 Patch Release 8 supports the following FortiOS versions:

- FortiOS v4.0 MR3 and all Patch Releases
- FortiOS v4.0 MR2 and all Patch Releases

FortiOS v4.0 MR2 is no longer supported (EOS) as of April 1, 2013.

FortiOS Carrier support

FortiAnalyzer v4.0 MR3 Patch Release 8 supports the following FortiOS Carrier versions:

- FortiOS Carrier v4.0 MR3 and all Patch Releases
- FortiOS Carrier v4.0 MR2 and all Patch Releases

FortiOS Carrier v4.0 MR2 is no longer supported (EOS) as of March 31, 2013.

FortiManager support

FortiAnalyzer v4.0 MR3 Patch Release 8 supports FortiManager v4.0 MR3.

FortiClient (Windows) support

FortiAnalyzer v4.0 MR3 Patch Release 8 supports FortiClient v4.0 MR2.

FortiClient v4.0 MR2 is no longer supported (EOS) as of May 14, 2013.

FortiMail support

FortiAnalyzer v4.0 MR3 Patch Release 8 supports FortiMail v4.0 MR3 Patch Release 3 or later.

FortiCache support

FortiAnalyzer v4.0 MR3 Patch Release 8 supports FortiCache v2.0 MR2.

FortiWeb support

FortiAnalyzer v4.0 MR3 Patch Release 8 supports FortiWeb v4.0 MR4 Patch Release 6.

MySQL Server support

FortiAnalyzer v4.0 MR3 Patch Release 8 supports MySQL Server v5.1.137.

On MySQL server, the administrator should grant privileges to FortiAnalyzer using the following commands:

```
grant all privileges on <database-name>.* to <username>@"<server-name>"
identified by 'password';
grant all privileges on <database-name>_hcache.* to
<username>@"<server-name>" identified by 'password';
```

Where, `server-name` is the domain name or IP address of the FortiAnalyzer device.

Virtualization software support

FortiAnalyzer v4.0 MR3 Patch Release 8 supports the following virtualization software:

- VMware ESX versions 4.0 and 4.1
- VMware ESXi versions 4.0, 4.1, 5.0, and 5.1

For more information, see FortiAnalyzer VM.

Language support

The following table lists FortiAnalyzer language support information.

Table 1: Language support

Language	Web-based Manager	Reports	Documentation
English	✔	✔	✔
French	-	✔	-
Spanish	✔	✔	-
Portuguese	-	✔	-
Korean	✔	✔	-
Chinese (Simplified)	✔	✔	-
Chinese (Traditional)	✔	✔	-
Japanese	✔	✔	-

To change the FortiAnalyzer language setting, go to *System* > *Admin* > *Settings*, in *Language Web Administration* select the desired language on the drop-down menu.

Resolved Issues

The resolved issues tables listed below do not list every bug that has been corrected with FortiAnalyzer v4.0 MR3 Patch Release 8 build 0719. The bug IDs are from Fortinet's internal bug tracking system. For inquires about a particular bug, please contact Customer Service & Support.

Logging

Table 2: Resolved logging issues

Bug ID	Description
0190689	Syslog messages are not displayed in the Web-based Manager.
0196770	The `diagnose fortilogd msgrate-device` CLI command displays incorrect output.
0200138	Syslog logs may be improperly inserted into the database when the logs contain control characters.
0201819	A generic syslog event forwarded from FortiAnalyzer is incorrectly formatted.
0201972	Spurious power supply failure messages may be reported by FortiAnalyzer.
0202911	FortiMail *Client_name* entries longer than 40 bytes are not inserted into the SQL database. The length definition has been changed to 256 bytes.
0203760	Event logs may be truncated when FortiAnalyzer retrieves logs from FortiGate.

Other

Table 3: Other resolved issues

Bug ID	Description
0214330	Added a continuous self-test to the RNG seed while it is running in FIPS-CC mode.
0220173	Foreign language support in PDF reports.

Reporting

Table 4: Resolved reporting issues

Bug ID	Description
0169197	User CN retrieval from the LDAP server may not be completed when multiple domain controllers are configured.
0196442	The report output displays a truncated filter list. The buffer length for the report filter has been changes to 1024 bytes which is the maximum length of a filter.

Known Issues

The known issues tables listed below do not list every bug that has been identified with FortiAnalyzer v4.0 MR3 Patch Release 8 build 0719. The bug IDs are from Fortinet's internal bug tracking system. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Logging

Table 5: Known logging issues

Bug ID	Description
0185330	The generic filter should work for syslog log messages.

Reporting

Table 6: Known reporting issues

Bug ID	Description
0196756	The default wireless report references to an incorrect log ID.

System Settings

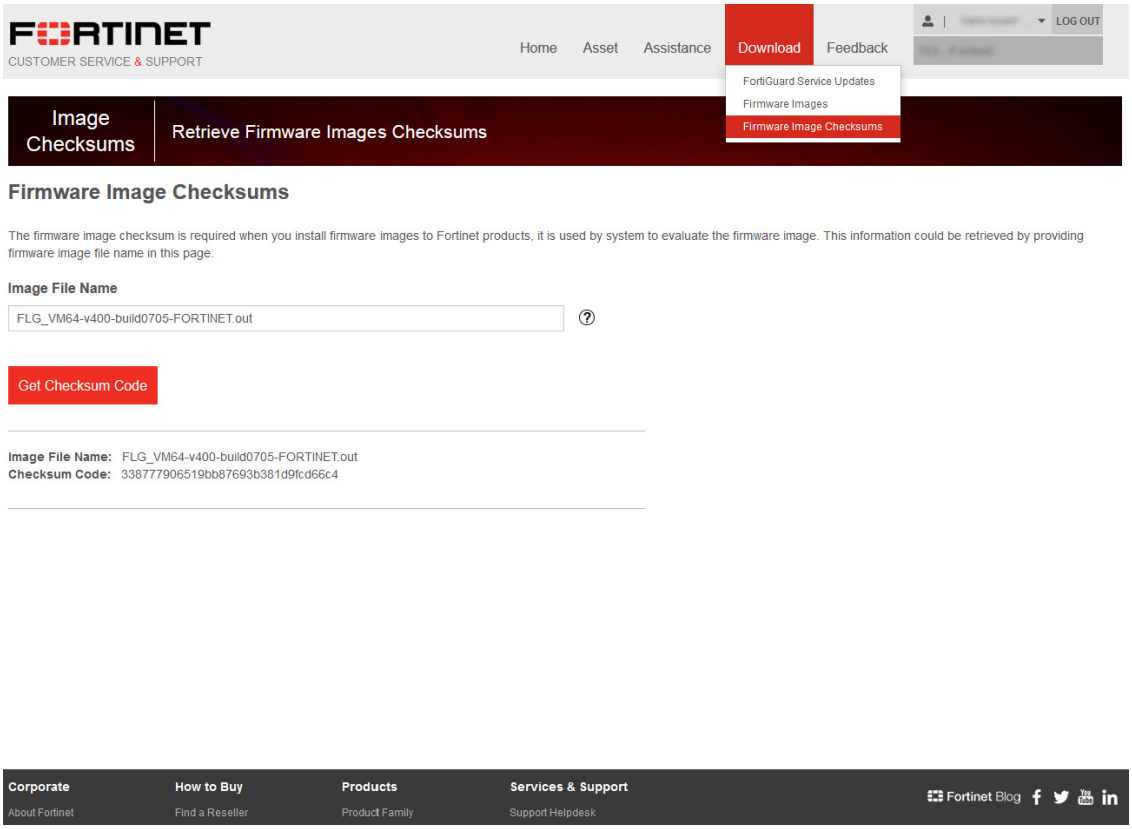
Table 7: Known system settings issues

Bug ID	Description
0174933	Software RAID displays an incorrect disk layout/number in the Web-based Manager and CLI.
0195136	Alertmail fails to resolve the mail server domain name.
0200515	The FAZ-2000A is not able to sustain the recommended log receive rate.

Firmware Image Checksums

The MD5 checksum code for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at https://support.fortinet.com. After logging in, select *Download* > *Firmware Image Checksums*, enter the image file including the extension, and select *Get Checksum Code*.

Figure 4: Firmware image checksum tool



Appendix A: FortiAnalyzer VM

FortiAnalyzer VM system requirements

The following table provides a detailed summary on FortiAnalyzer VM system requirements.

Table 8: FortiAnalyzer VM system requirements

Virtual Machine	Requirement
Hypervisor Support	VMware ESX versions 4.0 and 4.1 VMware ESXi versions 4.1, 5.0, and 5.1
Virtual Machine Form Factor	Open Virtualization Format (OVF)
Maximum Virtual CPUs Supported	Unlimited
Virtual NICs Required (Minimum / Maximum)	1 / 4
Virtual Machine Storage Required (Minimum / Maximum)	80GB / 2TB
Virtual Machine Memory Required (Minimum / Maximum)	1GB / 4GB
High Availability Support	Yes

FortiAnalyzer VM licence enhancements

The following enhancements have been made to FortiAnalyzer VM:

- Stackable license model for FAZ-VM

  The following table details FortiAnalyzer VM v5.0 to v4.0 MR3 license conversions.

  Table 9: FortiAnalyzer VM license conversion table

FortiAnalyzer VM version 5.0 license SKU	FortiAnalyzer version 4.0 MR3 license SKU
FAZ-VM-BASE + 4x FAZ-VM-GB1	FAZ-VM-100
FAZ-VM-BASE + 4x FAZ-VM-GB1 or FAZ-VM-BASE + 1x FAZ-VM-GB5	FAZ-VM-400
FAZ-VM-BASE + 1x FAZ-VM-GB25	FAZ-VM-1000
FAZ-VM-BASE + 2x FAZ-VM-GB25	FAZ-VM-2000
FAZ-VM-BASE + 1x FAZ-VM-GB100	FAZ-VM-4000
FAZ-VM-BASE + 2x FAZ-VM-GB100	FAZ-VM-UNL

For more information see the FortiAnalyzer product datasheet available on the Fortinet web site, http://www.fortinet.com/products/fortianalyzer/index.html.

FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer VM firmware images in two formats:

- `.out`: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `ovf.zip`: Download either the 32-bit or 64-bit package for a new FortiAnalyzer VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.