FortiAnalyzer v5.0 Patch Release 1
Release Notes

FortiAnalyzer v5.0 Patch Release 1 Release Notes

October 15, 2013

05-501-188070-20131015

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
2012-11-22	Initial release.
2012-11-22	Removed 178640, 187453, and 185283 from Known Issues.
2012-11-23	Added note to upgrade chapter. Added information on downgrading to previous versions.
2012-11-26	Updated the Upgrade Information section for FortiAnalyzer VM upgrades.
2012-11-30	Added 188237 to known upgrade issues.
2012-12-03	Updated table 1 Device limits to include older FortiAnalyzer hardware.
2012-12-21	Updated *Upgrade Information* > *FortiAnalyzer VM license*.
2013-02-27	Minor update to product integration and support chapter.
2013-04-12	Minor update to upgrade information chapter.
2013-05-14	Minor document update.
2013-10-09	Added a FortiAnalyzer VM upgrade warning to the Upgrade Information chapter and added note in Special Notices.
2013-10-15	Updated FortiAnalyzer VM upgrade warning.

Introduction

This document provides a summary of new features, support information, installation instructions, integration, resolved and known issues in FortiAnalyzer v5.0 Patch Release 1.

Supported models

The following models are supported on FortiAnalyzer v5.0 Patch Release 1.

FortiAnalyzer

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

FortiAnalyzer VM

FAZ-VM32 and FAZ-VM64.

See http://docs.fortinet.com/fa.html for additional documents on FortiAnalyzer v5.0.

Summary of enhancements

The following is a list of enhancements in FortiAnalyzer v5.0 Patch Release 1:

- Added support for IPv6 networking
- Auto-generate log fields
- Certificate compatibility with FortiGate
- Dataset improvements
- Device Manager
- FortiOS v5.0.0 support
- GTP log compatibility
- Improved Collector and Analyzer modes
- Log Aggregation (Collector mode)
- Multiple concurrent running reports
- New DVM table
- New FortiAnalyzer VM licensing model
- New PDF report style
- Real-time Monitoring (RTM)
- Removed index-based logging and reporting
- Support OU for the report LDAP filter
- Support upgrade from FortiAnalyzer v4.0 MR3

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer v5.0 Patch Release 1.

FortiAnalyzer VM upgrade

In FortiAnalyzer v4.0 MR3, the Open Virtualization Format (OVF) setting uses 2 virtual CPUs, however v5.0 uses 1 virtual CPU. It is essential to change the vCPU setting to 1 before upgrading your FortiAnalyzer VM to avoid server instability or other serious issues.

Fortinet recommends upgrading to the latest VMware ESXi 4.1 Patch Release before upgrading FortiAnalyzer VM or changing the vCPU setting. If ESXi server instability or PSOD issue persists, please contact VMware support for proper guidance.

CLI commands

In FortiAnalyzer v5.0 Patch Release 1, all system related features are configured via `config fmsystem`. Other features are configured via `config fasystem`.

Device manager

The FortiAnalyzer v5.0 Patch Release 1 release includes a device manager to manage the FortiGate and FortiCarrier devices that are logging to it.

Upgrade Information

Upgrading from FortiAnalyzer v4.0 MR3

FortiAnalyzer v5.0 Patch Release 1 build 0087officially supports upgrade from FortiAnalyzer v4.0 MR3 Patch Release 5 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 v5.0 Patch Release 1 Administration Guide* at http://docs.fortinet.com.

Upon upgrading to FortiAnalyzer v5.0 Patch Release 1, the system automatically begins converting the v4.0 MR3 logs, and inserts them into the SQL database. An icon appears at the top right corner after login to the Web-based Manager next to the logout and help buttons. This pops-up a small window displaying the progress.

Upon upgrading from FortiAnalyzer v4.0 MR3 the Web-based Manager incorrectly reports that the device is downgrading the firmware version. If you upgrade the firmware version from the CLI using the `execute restore all-settings` CLI command, the message is correct.

In FortiAnalyzer v4.0 MR3, the Open Virtualization Format (OVF) setting uses 2 virtual CPUs, however v5.0 uses 1 virtual CPU. It is essential to change the vCPU setting to 1 before upgrading your FortiAnalyzer VM to avoid server instability or other serious issues.

Fortinet recommends upgrading to the latest VMware ESXi 4.1 Patch Release before upgrading FortiAnalyzer VM or changing the vCPU setting. If ESXi server instability or PSOD issue persists, please contact VMware support for proper guidance.

FortiAnalyzer VM license

Upgrading a FortiAnalyzer VM device from v4.0 MR3 Patch 5 (and above) to v5.0 Patch Release 1 is supported. The old VM license is converted into the new VM stackable license model. New VM installations running v5.0 Patch Release 1 can be deployed with the .ovf file and application of either an old v4.0 MR3 or new v5.0 license.

Supported configuration

The following configurations are retained after upgrade:

- `host name`
- `config system interface`
- `config system route`
- `config system dns`
- `config system sql`
- `config log setting`

Aggregation and Collector mode configuration

Aggregation and Collector mode configurations are retained after upgrade.

Device

FortiGate and FortiCarrier devices are supported in FortiAnalyzer v5.0 Patch Release 1, and are retained after upgrade. Other devices are not yet supported in FortiAnalyzer v5.0.

FortiGate High Availability (HA) clusters

After the system finishes upgrading, FortiGate HA clusters are split into individual devices in the device manager (master + slaves). They appear as standalone devices. This may cause the maximum number of allowed devices to be reached since in FortiAnalyzer v4.0 MR3 HA clusters are counted as one device. Secure logging from a FortiGate HA cluster to a FortiAnalyzer device using IPsec VPN has inconsistent connectivity upon failover of the HA cluster.

Log

All raw log files are retained upon upgrade for FortiGate, FortiCarrier, and FortiMail devices. However, the logs for FortiMail are unable to be viewed in the Log View.

Partially supported configuration

Administrative Domains (ADOMs)

If ADOMs are enabled in FortiAnalyzer v4.0 MR3, after the upgrade the ADOMs are re-created but the FortiGate devices are not assigned to an ADOM. FortiAnalyzer v5.0 allows for a device to assigned to only one ADOM.

Device group

Only those device groups in the root ADOM are retained after upgrade. Selecting a device group in a report, log view, or the RTM profile is not yet supported in FortiAnalyzer v5.0.

Log report

FortiAnalyzer v5.0 Patch Release 1 only supports PDF reports. FortiAnalyzer v4.0 MR3 PDF reports can be seen in *Report History* after upgrade.

Unsupported configuration

The following configurations are not retained and must be re-created after upgrade.

- RADIUS server
- TACACS+ server
- Authentication group
- Admin users
- Profiles
- Pre-login banner
- After-login banner
- SNMP settings
- Alert event
- Syslog server
- Default device allocation space
- Report remote output
- Per device IPsec tunnel configuration

FortiAnalyzer v4.0 MR3 Report layouts, charts, and datasets are not supported.

Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous FortiAnalyzer firmware release via the Web-based Manager or CLI. FortiAnalyzer. A system reset is required after the firmware downgrading process has completed.

All configuration will be lost after downgrading the device. For FortiAnalyzer devices with hard drives installed, the hard drives will be formatted.

To re-initialize a FortiAnalyzer, use the following CLI commands via a console port connection:

```
execute reset all-settings
esecute format disk
```

Product Integration and Support

Web browser support

FortiAnalyzer v5.0 Patch Release 1 supports the following web browsers:

- Microsoft Internet Explorer version 9
- Mozilla Firefox versions 15 and 16

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

FortiOS support

FortiAnalyzer v5.0 Patch Release 1 supports the following FortiOS versions:

- FortiOS v5.0.0 release or later
- FortiOS v4.0 MR3 Patch Release 2 or later
- FortiOS v4.0 MR2 and all Patch Releases

FortiOS Carrier support

FortiAnalyzer v5.0 Patch Release 1 supports the following FortiOS Carrier versions:

- FortiOS Carrier v5.0.0 release or later
- FortiOS Carrier v4.0 MR3 Patch Release 2 or later
- FortiOS Carrier v4.0 MR2 and all Patch Releases

FortiMail support

FortiAnalyzer v5.0 Patch Release 1 does not support FortiMail logging. Support will be added in a future release.

FortiSwitch support

FortiAnalyzer v5.0 Patch Release 1 does not support FortiSwitch logging.

Language support

FortiAnalyzer v5.0 Patch Release 1 is localized for the following languages:

Language	Web-based Manager	Documentation
English	Yes	Yes
Korean	Yes	-
Chinese (Simplified)	Yes	-
Chinese (Traditional)	Yes	-
Japanese	Yes	-

To change the FortiGate language setting, go to *System Settings* > *Admin* > *Admin Settings*, under *Administrative Settings* > *Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Supported models

The following tables list which FortiGate and FortiCarrier models and firmware versions can log to a FortiAnalyzer appliance running FortiAnalyzer v5.0 Patch Release 1. Please ensure that the devices that you manage are supported before completing the upgrade.

Table 1: Supported FortiGate models

Model	Firmware Version
FG-20C, FG-20C-ADSL-A, FG-40C, FG-60C, FG-60D, FG-60C-POE, FG-80C, FG-80CM, FG-100D, FG-110C, FG-111C, FG-200B, FG-200B-POE, FG-300C, FG-310B, FG-310B-DC, FG-311B, FG-600C, FG-620B, FG-620B-DC, FG-621B, FG-800C, FG-1000C, FG-1240B, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3810A, FG-3950B, FG-3951B, FG-5001B, FG-5101C FG-VM32, FG-VM64 FWF-20C, FWF-20C-ADSL-A, FWF-40C, FWF-60C, FWF-60D, FWF-60CM, FWF-60CX-ADSL-A, FWF-80CM, FWF-81CM FS-5203B	v5.0

Table 1: Supported FortiGate models

Model	Firmware Version
FG-20C, FG-20C-ADSL-A, FG-30B, FG-40C, FG-50B, FG-51B, FG-60B, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60CM, FG-80C, FG-80CM, FG-82C, FG-100A, FG-100D, FG-110C, FG-111C, FG-200A, FG-200B, FG-200B-POE, FG-224B, FG-300A, FG-300C, FG-310B, FG-310B-DC, FG-311B, FG-400A, FG-500A, FG-600C, FG-620B, FG-620B-DC, FG-621B, FG-800, FG-800C, FG-800F, FG-1000, FG-1000A, FG-1000A-FA2, FG-1000C, FG-1240B, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600, FG-3600A, FG-3810A, FG-3950B, FG-3951B, FG-5001, FG-5001A, FG-5001B, FG-5001C, FG-5001FA2, FG-5002FB2, FG-5005FA2, FG-5101C, FG-ONE FG-VM32, FG-VM64, FG-VM64-XEN FGR-100C FWF-20C, FWF-20C-ADSL-A, FWF-30B, FWF-40C, FWF-50B, FWF-60B, FWF-60C, FWF-60CM, FWF-60CM-3G4G-B, FWF-60CX-ADSL-A, FWF-80CM, FWF-81CM FS-5203B	v4.0 MR3
FG-30B, FG-50B, FG-51B, FG-60-ADSL, FG-60B, FG-60C, FG-60CM, FG-80C, FG-80CM, FG-82C, FG-100A, FG-110C, FG-200A, FG-200B, FG-200B-POE, FG-224B, FG-300A, FG-300C, FG-310B, FG-310B-DC, FG-311B, FG-400A, FG-500A, FG-620B, FG-620B-DC, FG-800, FG-800F, FG-1000, FG-1000A, FG-1000A-FA2, FG-1240B, FG-3000, FG-3016B, FG-3040B, FG-3140B, FG-3600, FG-3600A, FG-3810A, FG-3950B, FG-3951B, FG-5001, FG-5001A, FG-5001B, FG-5001FA2, FG-5002FB2, FG-5005FA2, FG-ONE FG-VM FWF-30B, FWF-50B, FWF-60B, FWF-60C, FWF-60CX-ADSL-A, FWF-80CM, FWF-81CM	v4.0 MR2

Table 2: Supported FortiCarrier models

Model	Firmware Version
FCR-3240C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C FCR-VM, FCR-VM64	v5.0
FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2	v4.0 MR3
FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2	v4.0 MR2

Resolved Issues

The resolved issues tables listed below do not list every bug that has been corrected with FortiAnalyzer v5.0 Patch Release 1 build 0087. For inquires about a particular bug, please contact Customer Service & Support.

Upgrade

Table 3: Resolved upgrade issues

Bug ID	Description
0187836	Support upgrade FortiAnalyzer from v4.0 MR3 to v5.0 Patch Release 1.

System Settings

Table 4: Resolved system settings issues

Bug ID	Description
0179292	The RAID Monitor widget displays an error message when the RAID level is set to RAID+spare, such as 1s, 5s, or 6s. However, the RAID level successfully is set.

Known Issues

The known issues tables listed below do not list every bug that has been identified with FortiAnalyzer v5.0 Patch Release 1 build 0087. 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
0178218	The FortiAnalyzer fails to open email archives from DLP logs.
0186601	FortiMail logs are unable to be viewed in the Log View.
0187459	Filter and search functionality fails for real time logs.
0188952	Secure logging from a FortiGate HA cluster to a FortiAnalyzer device using IPsec has inconsistent connectivity upon failover of the HA cluster.
0189346	Collector mode: After upgrading from v4.0 MR3, FortiAnalyzer should not display the SQL database upgrade icon.

Real-time Monitor

Table 6: Known real-time monitor issues

Bug ID	Description
0187569	The RTM timestamps displayed at the bottom of the chart are crowded.

Reporting

Table 7: Known reporting issues

Bug ID	Description
0186525	The FortiAnalyzer may fail to produce charts for *Top Allowed Websites by Bandwidth*, *Top Viruses by Name*, or *Top Viruses Victims*.
0187482	The column setting is unavailable in the chart page when chart type is set to table.
0187529	An output profile is able to be created but can not be edited.
0187657	When creating new schedules, if you choose *Specify* but do not select any device and click OK, FortiAnalyzer will silently drop the configuration.
0187781	An improperly configured chart may cause the SQL report daemon *run_sql_rpt* to crash.

Table 7: Known reporting issues (continued)

Bug ID	Description
0188705	Internet Explorer 9 issue. When creating a new report schedule chart dataset etc, you need to close the browser and re-open. You can then can see the newly created chart.
0189386	When editing a report schedule, the Web-based Manager device selection display will be changed to *Specify* when the backend configuration is *All FortiGate.*

System Settings

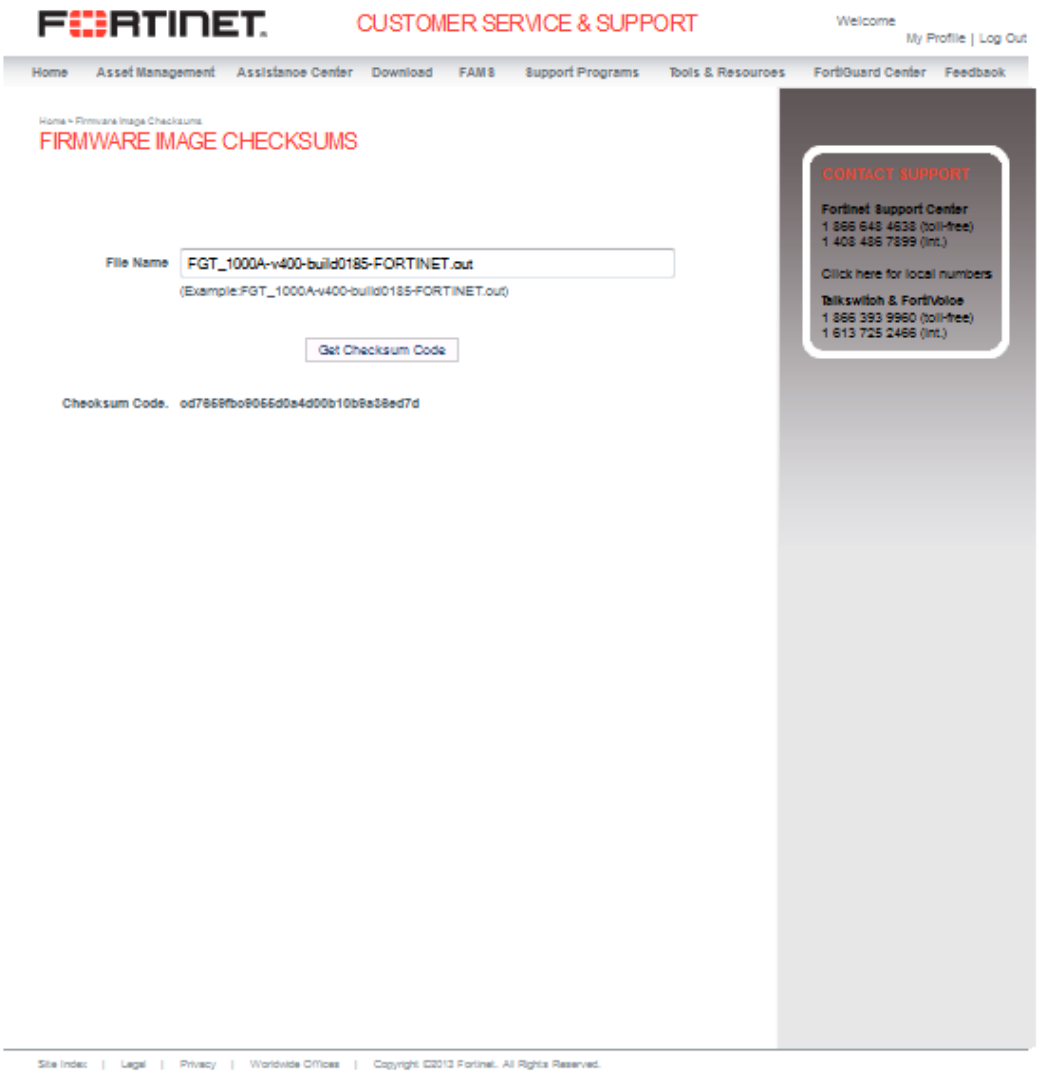
Table 8: Known system settings issues

Bug ID	Description
0179217	FortiAnalyzer v5.0 Patch Release 1 supports FortiGate and FortiCarrier logging only. Support for other devices will be added in future releases.
0180601	FortiAnalyzer v5.0 Patch Release 1 does not support the functionality to backup and restore logs and archives.
0183094	The Web-based Manger inadvertently displays a pop message when a device is promoted.
0184590	The FortiAnalyzer does not support automatic registration of devices.
0187074, 0189052	The RAID array may fail if at least one disk works intermittently.
0187075	An error message is displayed upon formatting the disks on a FAZ-2000B or FAZ-4000B. However, the disk is formatted successfully.
0187518	The *ddmd* daemon may consume the CPU resources.

Firmware Image Checksums

The MD5 checksums 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 Checksum*, enter the image file including the extension, and select *Get Checksum Code*.

Figure 1: 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 9: FortiAnalyzer VM system requirements

Virtual Machine	Requirement
Hypervisor Support	VMware ESX versions 4.0 and 4.1 VMware ESXi versions 4.0, 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

FortiAnalyzer VM licence enhancements

With FortiAnalyzer v5.0 Patch Release 1, the following changes have been made to FortiAnalyzer VM:

- Stackable license model for FortiAnalyzer VM license add-ons

SKU	Description
FAZ-VM-BASE	Basic license includes 1GB/Day of logs, and 200GB device quota storage.
FAZ-VM-GB1	Additional 1GB/Day of logs, and an additional 200GB device quota storage.
FAZ-VM-GB5	Additional 5GB/Day of logs, and an additional 1TB device quota storage
FAZ-VM-GB25	Additional 25GB/Day of logs, and an additional 8TB device quota storage
FAZ-VM-100	Additional 100GB/Day of logs, and an additional 16TB device quota storage

- License information is displayed on dashboard
- Device Quota Storage/Device Quota Storage Used displayed on dashboard.

Appendix B: FortiAnalyzer Device Limits

FortiAnalyzer device limits

The following table outlines the device limits for FortiAnalyzer v5.0 Patch Release 1.

Table 10: FortiAnalyzer device limits

Model	Maximum Log Rate (Log/Second)	Supported Devices/ADOMs (Maximum)	GB/Day of logs
FAZ-100C	350	150	5GB
FAZ-200D	350	150	5GB
FAZ-400B	625	200	15GB
FAZ-400C	625	200	15GB
FAZ-1000B	1000	2000	25GB
FAZ-1000C	1000	2000	25GB
FAZ-2000A	3000	2000	75GB
FAZ-2000B	3000	2000	75GB
FAZ-4000A	6000	2000	150GB
FAZ-4000B	6000	2000	150GB
FAZ-VM-Base	6000	10000	1GB
FAZ-VM-GB1	6000	10000	+1GB
FAZ-VM-GB5	6000	10000	+5GB
FAZ-VM-GB25	6000	10000	+25GB
FAZ-VM-GB100	6000	10000	+100GB

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