FortiAnalyzer v5.0 Patch Release 3
Release Notes

FortiAnalyzer v5.0 Patch Release 3 Release Notes

October 15, 2013

05-503-204898-20131015

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
2013-07-10	Initial release.
2013-07-29	Added Google Chrome to supported web browsers. Removed 0193937 from known issues. Added 0212512 and 0212446 to Known Issues chapter.
2013-08-06	Updated web browser support information.
2013-08-27	Updated FortiOS support information. Added 0213707 to Known Issues chapter.
2013-09-26	Added the FAZ-1000D to supported models.
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 enhancements, support information, installation instructions, integration, resolved and known issues in FortiAnalyzer v5.0 Patch Release 3 build 0200. Please review all sections in this document prior to upgrading your device. For more information on upgrading your FortiAnalyzer device, see the *FortiAnalyzer v5.0 Patch Release 3 Administration Guide*.

This document includes the following sections:

Supported models

The following models are supported on FortiAnalyzer v5.0 Patch Release 3.

FortiAnalyzer

FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-4000A, and FAZ-4000B.

FAZ-1000D

This model is released on a special branch based off of FortiAnalyzer v5.0 Patch Release 3. As such, the build number found in the *System Settings* > *Dashboard* page and the output from the `get system status` CLI command displays `4024` as the build number.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a `Branch point` field that should read `0200`.

FortiAnalyzer VM

FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.

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 3:

- Log search
- Device storage and log management
- RAID management
- Report Web-based Manager enhancements
- Merge event log based charts to the default report
- Chart level filters
- Report filter improvements
- Drill Down tab
- Event Management tab
- FortiMail logging and reporting support
- FortiWeb logging and reporting support
- FortiAnalyzer VM support for Microsoft Hyper-V Server
- Added support for real-time syslog forwarding over TCP connections
- Web Filter report template
- WiFi Network Summary report template

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer v5.0 Patch Release 3 build 0200.

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.

Pre-processing logic of ebtime

Logs with the following conditions met are considered usable for the calculation of estimated browsing time:

Traffic logs with `logid` of `13` or `2`, when `logid == 13`, `hostname` must not be empty. The `service` field should be either `HTTP`, `80/TCP` or `443/TCP`.

If all above conditions are met, then `devid`, `vdom`, and `user` (`srcip` if `user` is empty) are combined as a key to identify a user. For time estimation, the current value of `duration` is calculated against history session start and end time, only un-overlapped part are used as the `ebtime` of the current log.

RTM profiles

RTM profiles have been removed in FortiAnalyzer v5.0 Patch Release 3. You can use the new Drill down feature to gather detailed information on log devices and log arrays. Drill down includes traffic, web, email, and threat activity.

FortiMail/FortiWeb logging and reporting support

FortiAnalyzer v5.0 Patch Release 3 introduces FortiMail and FortiWeb logging and reporting support. ADOMs must be enabled on FortiAnalyzer before these devices can be added. FortiMail and FortiWeb are log triggered devices. Once configured to log to the FortiAnalyzer they will be displayed in the unregistered device list. Upon promoting the device to the DVM table, it will be added to the respective default ADOM.

FortiMail and FortiWeb devices cannot be manually added using the Add Model Device wizard.

FortiSwitch support

FortiAnalyzer v5.0 Patch Release 1 or later does not support FortiSwitch for logging and reporting.

Device groups

Device groups are not supported in FortiAnalyzer v5.0 Patch Release 2 or later. Device group configuration will be removed upon upgrade. You can use the new log array feature to group managed devices into groups for logging and reporting. Log arrays are configured at the ADOM level, but when scheduling reports you can select to run reports against multiple managed devices or multiple log arrays. The device raw log files and log SQL database are retained after upgrade. If you move a device to a log array after the upgrade, FortiAnalyzer will stop logging entries in the device log SQL database and start logging entries in a new log array SQL database. See the *FortiAnalyzer v5.0 Patch Release 3 Administration Guide* for more information.

Log arrays

After creating a log array, only new logs will be populated into this array. Older logs will remain on the device. To collect older logs, you will need to build the array database. Use the following CLI command to build the array database:

```
execute sql-local rebuild-device <log array device ID>
```

The SQL logs for the members of the log array will be rebuilt. To verify that the array rebuild was successful, select the Log View tab to view the log array and logs.

Executing this command will not reboot the FortiAnalyzer device.

Fortinet recommends configuring log arrays prior to deploying the FortiAnalyzer into production. When adding and deleting log arrays, you will need to rebuild the database to view older logs.

FortiAnalyzer VM license check

As a part of the license validation process FortiAnalyzer VM compares its IP addresses with the IP information in the license file. If the IP addresses do not match, FortiAnalyzer VM returns the error `IP does not match` within CLI command `get system status` output. If a new license has been imported or the FortiAnalyzer VM's IP address has been changed, the FortiAnalyzer VM must be manually rebooted in order for the system to validate the change and operate with a valid license.

Extended UTM log for Application Control

Upon upgrading to FortiAnalyzer v5.0 Patch Release 1 or later the application control log is not visible until you enable the extended UTM log in the FortiOS CLI.

To enable extended UTM log, use the following CLI command:

```
config application list
  edit <name>
    set extended-utm-log enable
end
```

ConnectWise Management Services Platform (MSP) support

ConnectWise Management Services Platform (MSP) is not supported FortiAnalyzer v5.0 Patch Release 1 or later. Upon upgrading to v5.0 Patch Release 1 or later, FortiAnalyzer ConnectWise functionality will be broken.

Distributed upgrades

For Collector/Analyzer architecture upgrades, Fortinet recommends upgrading the Analyzer first.

Upgrading the Collector first could impact the Analyzer's performance.

Report templates

When upgrading from FortiAnalyzer v4.0 MR3 to v5.0 Patch Release 1 or later, most report templates and customized reports will be removed. You will need to recreate these reports after upgrading.

Upgrade Information

Upgrading from FortiAnalyzer v5.0 Patch Release 1 or later

FortiAnalyzer v5.0 Patch Release 3 build 0200 officially supports upgrade from FortiAnalyzer v5.0 Patch Release 1 or Patch Release 2.

When upgrading a FAZ-300D to v5.0 Patch Release 3, you must first upgrade to v5.0 Patch Release 2.

Please review the Special Notices, Product Integration and Support, and Resolved Issues chapters prior to upgrading. For more information on upgrading your FortiAnalyzer device, see the *FortiAnalyzer v5.0 Patch Release 3 Administration Guide* at http://docs.fortinet.com.

You can download the Fortinet FortiManager-FortiAnalyzer MIB file in the firmware image FTP directory. The Fortinet Core MIB file is located in the main FortiAnalyzer v5.00 directory.

Upgrading from FortiAnalyzer v4.0 MR3

Fortinet recommends upgrading to FortiAnalyzer v5.0 Patch Release 1 build 0087 before upgrading to FortiAnalyzer v5.0 Patch Release 3.

Upon upgrading to FortiAnalyzer v5.0 Patch Release 1, your v4.0 MR3 logs are automatically converted and inserted 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` 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 6 or later to v5.0 Patch Release 3 is supported. The old VM license is converted into the new VM stackable license model. New VM installations running v5.0 Patch Release 3 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, FortiCarrier, FortiMail, and FortiWeb devices are supported in FortiAnalyzer v5.0 Patch Release 3, 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.

Log report

FortiAnalyzer v5.0 Patch Release 3 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
- Post-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.

General firmware upgrade steps

The following table lists the general firmware upgrade steps.

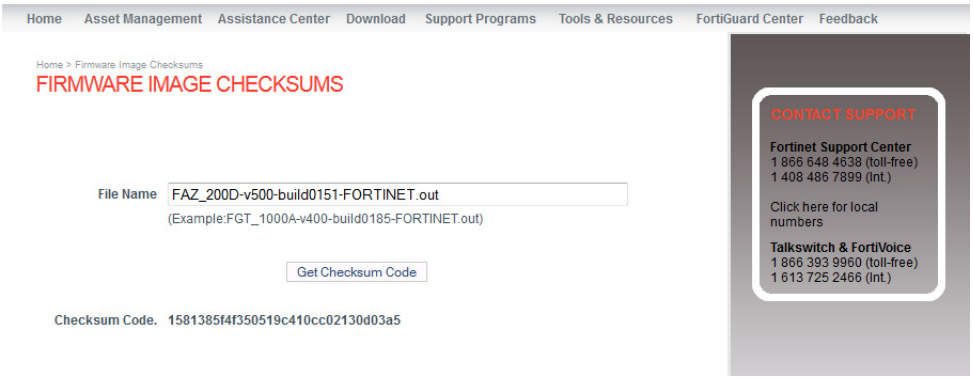
Table 1: Upgrade steps

Step 1	Prepare your FortiAnalyzer for upgrade.
Step 2	Backup your FortiAnalyzer system configuration. For FortiAnalyzer VM, take a *Snapshot* of the VM instance.
Step 3	Transfer the firmware image to your FortiAnalyzer device.
Step 4	Log into your FortiAnalyzer Web-based Manager to verify the upgrade was successful.

Step 1: Prepare your FortiAnalyzer for upgrade

1. Make sure all log devices are running the supported firmware version as stated in the Release Notes.
2. To verify the integrity of the download, go back to the *Download* section of the login page, then select the *Firmware Image Checksums* link.

Figure 1: Firmware image checksums page



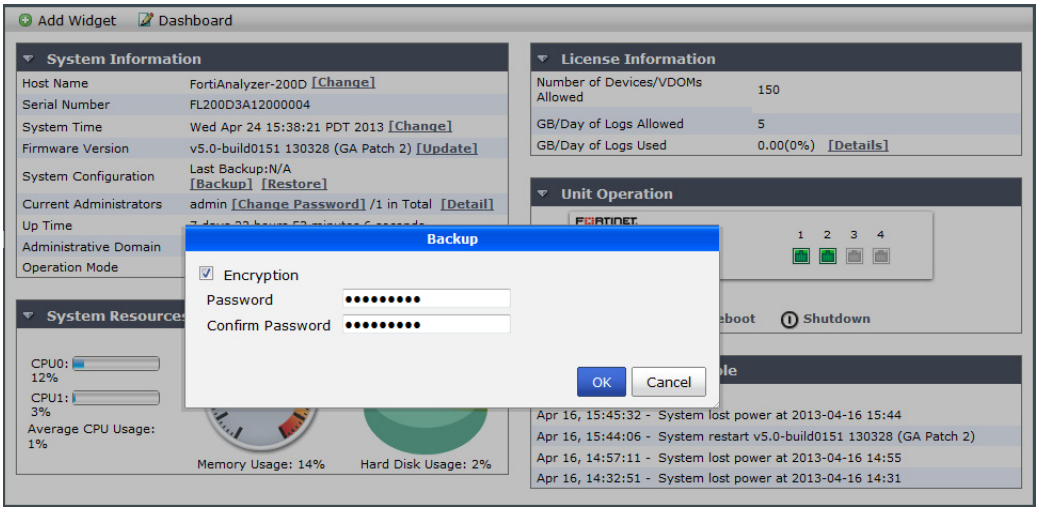
3. Enter the file name and select *Get Checksum Code* to get the firmware image checksum code. Compare this checksum with the checksum of the firmware image.

Step 2: Back up your FortiAnalyzer configuration

1. Go to *System Settings* > *General* > *Dashboard*.
2. In the *System Information* widget, under *System Configuration*, select *Backup*.

   The *Backup* dialog box opens.

Figure 2: Backup dialog box



3. Select the checkbox to encrypt the backup file and enter a password.

When selecting to encrypt the backup configuration file, the same password used to encrypt the file will be required to restore this backup file to the FortiAnalyzer device.

4. Select *OK* and save the backup file on your local computer.

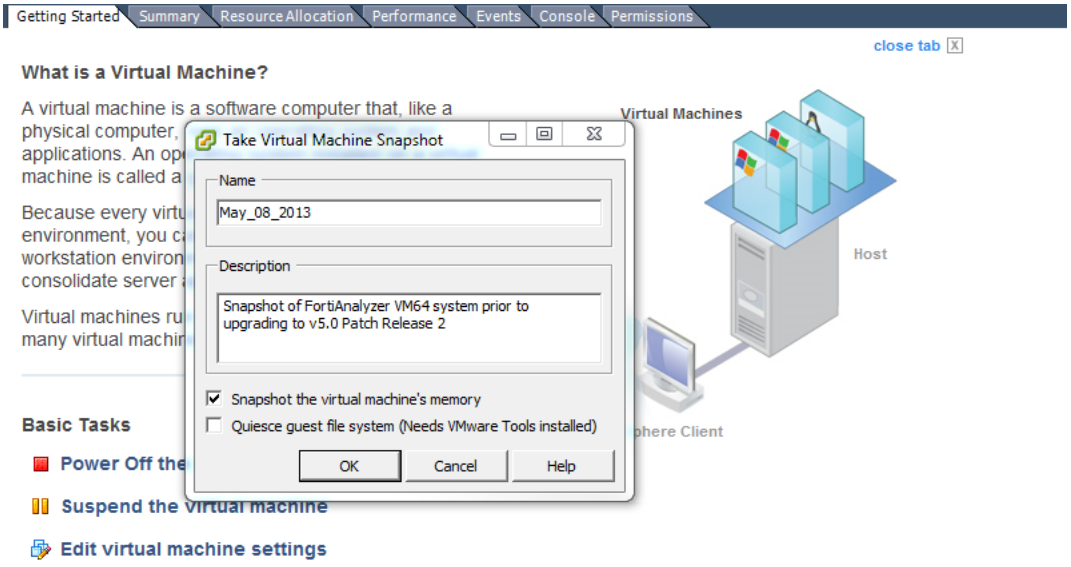
The system configuration file from a FortiAnalyzer v4.0 MR3 device cannot be directly imported into a FortiAnalyzer v5.0 Patch Release 3 device.

Optionally, you can backup the configuration file to a FTP, SFTP, or SCP server using the following CLI command:

```
execute backup all-settings {ftp | sftp} <server IP address>
    <path/filename to the server> <user name on server> <password>
    [cryptpasswd]
execute backup all-settings scp <server IP address> <path/filename to
    the server> <user name on server> <SSH certificate> <crptpassrd>
```

5. In VM environments, it is recommended that you take a *Snapshot* of the VM instance. In the event of an issue with the firmware upgrade, use the *Snapshot Manager* to revert to the *Snapshot*. To create a *Snapshot*, right-click the VM instance and select *Snapshot* > *Take Snapshot*.

Figure 3: Snapshot of FortiAnalyzer VM



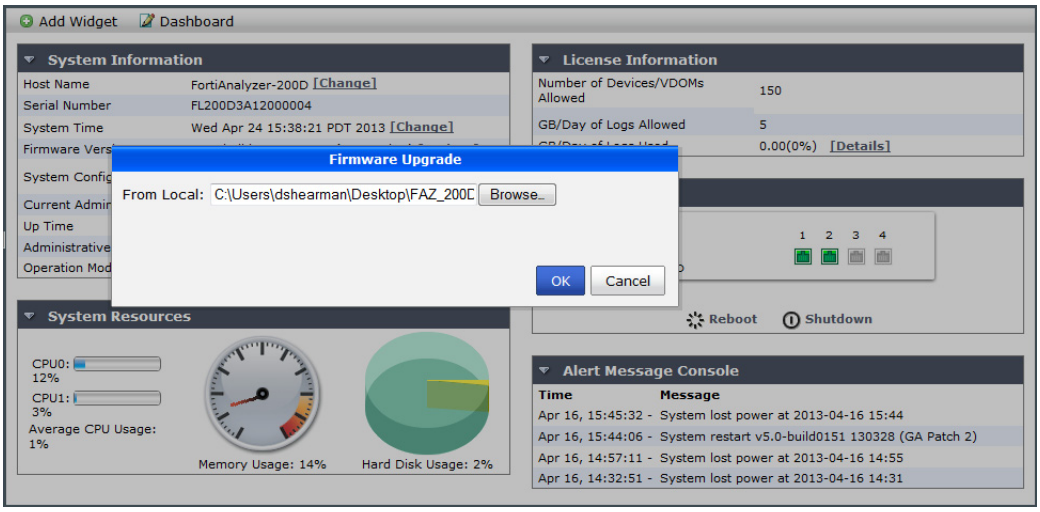
For information on snapshots in Microsoft Hyper-V Server environments, refer to the Microsoft Windows Server online help.

Step 3: Transfer the firmware image to your FortiAnalyzer device

1. Go to *System Settings* > *General* > *Dashboard*.
2. In the *System Information* widget, in the *Firmware Version* field, select *Update*.

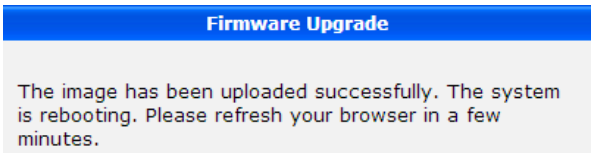
   The *Firmware Upgrade* dialog box opens.

Figure 4: Firmware upgrade dialog box



3. Select *Browse* to locate the firmware image (`.out` file) that you downloaded from the Customer Service & Support portal and select *Open*.
4. Select *OK. Your* FortiAnalyzer will upload the firmware image and you will receive the following message.

Figure 5: Firmware upgrade successful dialog box



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

```
exexute restore image {ftp | tftp} <file path on the FTP server>
     <server IP address <user name on server> <password>
```

Step 4: Verify the upgrade

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

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. A system reset is required after the firmware downgrading process has completed.

All configuration will be lost after downgrading the device and the hard drives could be formatted automatically.

Firmware downgrade is not recommended as it could lead to log data loss.

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

```
execute reset all-settings
execute format {disk | disk-ext4}
```

Product Integration and Support

Web browser support

FortiAnalyzer v5.0 Patch Release 3 supports the following web browsers:

- Microsoft Internet Explorer versions 9 and 10
- Mozilla Firefox version 24
- Google Chrome version 30

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

FortiOS support

FortiAnalyzer v5.0 Patch Release 3 supports the following FortiOS versions:

- FortiOS v5.0.0 and Patch Releases 1 to 3
- FortiOS v4.0 MR3 Patch Release 2 or later
- 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 v5.0 Patch Release 3 supports the following FortiOS Carrier versions:

- FortiOS Carrier v5.0.0 and Patch Releases 1 to 3
- FortiOS Carrier v4.0 MR3 Patch Release 2 or later
- FortiOS Carrier v4.0 MR2 and all Patch Releases

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

FortiMail support

FortiAnalyzer v5.0 Patch Release 3 supports the following FortiMail versions:

- FortiMail v5.0 Patch Release 1

In order for FortiMail devices to be promoted to the DVM table, ADOMs must be enabled. FortiMail devices are added to the default FortiMail ADOM.

FortiWeb support

FortiAnalyzer v5.0 Patch Release 3 supports the following FortiWeb versions:

- FortiWeb v5.0.0

In order for FortiWeb devices to be promoted to the DVM table, ADOMs must be enabled. FortiWeb devices are added to the default FortiWeb ADOM.

FortiSwitch support

FortiAnalyzer v5.0 Patch Release 3 does not support FortiSwitch logging.

FortiClient support

FortiAnalyzer v5.0 Patch Release 3 supports the following FortiClient versions:

- FortiClient (Windows) v5.0 Patch Release 4 or later
- FortiClient (Mac OS X) v5.0 Patch Release 4 or later

MySQL server support

FortiAnalyzer v5.0 Patch Release 3 supports MySQL Server v5.5.

Virtualization software support

FortiAnalyzer v5.0 Patch Release 3 supports the following virtualization software:

- VMware ESX versions 4.1
- VMware ESXi versions 4.1 and 5.1
- Microsoft Hyper-V Server 2008 and 2012

Other virtualization software versions may function correctly, but are not supported by Fortinet. See “FortiAnalyzer VM” for more information.

Language support

The following table lists FortiAnalyzer language support information.

Table 2: Language support

Language	Web-based Manager	Reports	Documentation
English	✔	✔	✔
French	-	See 0197460.	-
Spanish	-	✔	-
Portuguese	-	✔	-
Korean	✔	✔	-
Chinese (Simplified)	✔	✔	-
Chinese (Traditional)	✔	✔	-
Japanese	✔	✔	-

To change the FortiAnalyzer language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *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, FortiCarrier, FortiMail, and FortiWeb models and firmware versions can log to a FortiAnalyzer appliance running v5.0 Patch Release 3. Please ensure that the log devices are supported before completing the upgrade.

Table 3: Supported FortiGate models

Model	Firmware Version
FG-20C, FG-20C-ADSL-A, FG-30D, FG-40C, FG-60C, FG-60D, FG-60C-POE, FG-80C, FG-80CM, FG-90D, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-200B, FG-200B-POE, FG-200D, FG-240D, 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-3600C, FG-3810A, FG-3950B, FG-3951B, FG-5001B, FG-5001C, FG-5101C FG-VM32, FG-VM64, FG-VM64-XEN FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-80CM, FWF-81CM, FWF-90D FS-5203B	v5.0

Table 3: Supported FortiGate models (continued)

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-VM32 FWF-30B, FWF-50B, FWF-60B, FWF-60C, FWF-60CX-ADSL-A, FWF-80CM, FWF-81CM	v4.0 MR2

Table 4: Supported FortiCarrier models

Model	Firmware Version
FCR-3240C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5101C FCR-VM32, 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

Table 5: Supported FortiMail models

Model	Firmware Version
FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000, FE-5001A, FE-5002B FE-VM64	v5.0 Patch Release 1

Table 6: Supported FortiWeb models

Model	Firmware Version
FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-4000D FWB-VM64	v5.0

Resolved Issues

The resolved issues tables listed below do not list every bug that has been corrected with FortiAnalyzer v5.0 Patch Release 3 build 0200. For inquires about a particular bug, please contact Customer Service & Support.

Logging

Table 7: Resolved logging issues

Bug ID	Description
0172792	Added a list of possible *log_field* options for log search.
0190689	Syslog messages are not displayed in the Web-based Manager.
0194012	Custom fields should be displayed in the *Log View* tab.
0194536	Old log files are written repeatedly to the FTP server everyday.
0200138	Syslog logs are improperly inserted to the database.
0201819	Generic syslog events forwarded from FortiAnalyzer are incorrectly formatted.
0203102	The real-time filter does not work.
0203333	All GTP fields should be properly displayed.
0206341	*Log View* is not able to display logs after importing v4.0 MR3 logs.
0208776	Unable to view email filter logs with unsupported characters.
0208780	The *from* and *to* DLP log fields are empty.
0210332	In *Log View*, the log search does not support unsupported characters.
0210333	The *Log Search History* window stays open unless user clicks on an entry.

Reporting

Table 8: Resolved reporting issues

Bug ID	Description
0154659	Added estimated browsing time feature.
0194687	The CLI command `execute sql-report run` does not list the schedule names.
0202743	It is not possible to apply a dataset variable to a chart when creating a report template.
0203060	Missing option to specify data binding.
0203061	Missing group by option in chart configuration.

Table 8: Resolved reporting issues (continued)

Bug ID	Description
0203092	Data is not correct in table ranked chart.
0203496	A cloned chart result is different in various reports.
0203751	When a long test query is started, there is no way to stop it. Added a query stop button.
0204055	Unable to generate the *Top Country by Bandwidth* report with bar chart.
0205359	Unable to generate reports for FortiGates running FortiOS v4.0 MR3 Patch Release 10.
0205625	A chart with space in the name will cause the chart not to be editable.
0211526	Text boxes in reports do not wrap text.
0211636	A web server error 500 is displayed when attempting to edit an unprotected chart.

System Settings

Table 9: Resolved system settings issues

Bug ID	Description
0168800	Added SNMP trap for CPU alert without NICE usage.
0202542	The SNMP sysObjectID in FortiAnalyzer v5.0 Patch Release 2 is different than FortiAnalyzer v4.0 MR3.
0202595	The `sqllogd` daemon crashes continuously with signal 6 and 11 errors.
0202921	When enabling collector mode without setting a remote server IP, a random IP will be set.
0203473	Firefox and Chrome do not work with an HTTPS connection to one FortiAnalyzer with one FortiGate.
0203759	The FortiAnalyzer should alert the administrator that the storage is not mountable.
0203891	After changing the HTTP port, the Web-based Manager login no longer functions.
0205115	An LDAP user can log in without entering a password.
0205959	The OFTPD daemon does not respond.
0209046	Unable to restore logs from an FTP server.
0210856	High memory usage when the FortiAnalyzer is in an idle state.

Known Issues

The known issues tables listed below do not list every bug that has been identified with FortiAnalyzer v5.0 Patch Release 3 build 0200. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Logging

Table 10: Known logging issues

Bug ID	Description
0202901	Log search does not return the proper information.
0203973	Some logs are sent as text while others are sent as binary.
0211587	There is no `log-integrity` CLI command.
0211733	FortiMail history log subject is displayed in html format.
0212228	The last page of log view displays the message *No records found*. Workaround: Rebuild the SQL database using the `execute sql-local rebuild-db` CLI command.
0212348	Log view timeframe function; issue with cache and initial display.
0212446	An administrator Web-based Manager login can fail when *Log View* > *Security* > *Intrusion Prevention* logs are viewed many times.
0212512	In the log detail panel, the archive tab does not show archived link for all log archive typed.

Reporting

Table 11: Known reporting issues

Bug ID	Description
0167549	PDF reports with Russian / Hebrew / Hungarian text are not rendered correctly.
0197325	Custom chart data type is missing.
0197460	FortiAnalyzer v5.0 does not currently support French language reports.
0203657	Cannot remove pie charts from the Top Destination Addresses charts.
0207408	Time filter scope does not work correctly for test queries.
0211597	A chart with invalid characters in its name is not editable.

Table 11: Known reporting issues (continued)

Bug ID	Description
0212311	Cloned UTM Security Report upgrade problem.
0213707	When cloning a dataset or chart, if the name contains a space, an improper dataset or chart is created and it can never be edited or deleted.

System Settings

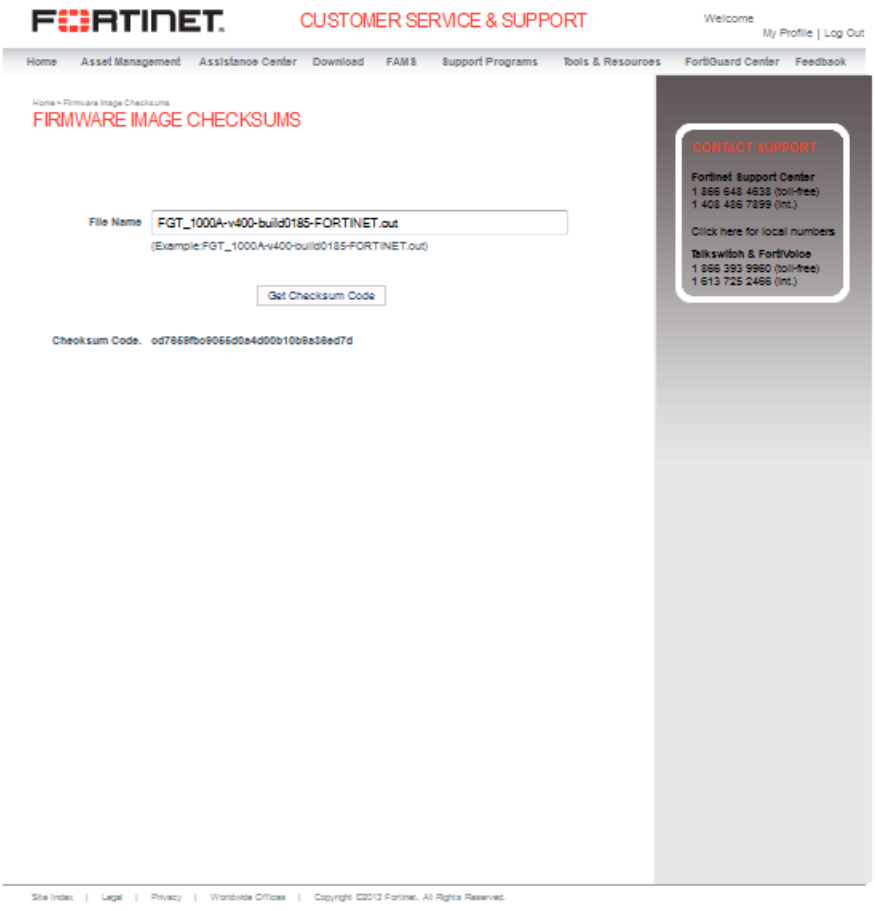
Table 12: Known system settings issues

Bug ID	Description
0209848	When promoting devices the available disk space is not checked.
0209980	For some double-PSU FortiAnalyzer models, when one PSU fails, there is no SNMP trap or local event log.
0211743	Alert events are not triggered for FortiMail or FortiWeb logs.
0212047	The FAZ-2000B only recognizes 4 CPU cores.
0212062	Log Aggregation does not work for FortiMail and FortiWeb devices.

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 6: Firmware image checksum tool



Appendix A: FortiAnalyzer VM

Licensing

Fortinet offers the FortiAnalyzer VM in a stackable license model based on GB logs per day and storage add-ons. This model allows you to expand your VM solution as your environment expands. When configuring your FortiAnalyzer, ensure to configure hardware settings as outlined in Table 13 and consider future expansion.

Table 13: FortiAnalyzer VM license information

Technical Specification	VM-Base	VM-GB1	VM-GB5	VM-GB25	VM-GB100
Hypervisor Support	VMware ESX versions 4.0 and 4.1 VMware ESXi versions 4.0, 4.1, 5.0 and 5.1 Microsoft Hyper-V Server 2008 and 2012				
VM Form Factor	VMware ESX/ESXi: Open Virtualization Format (OVF) Microsoft Hyper-V Server: Virtual Hard Disk (VHD)				
Devices / ADOMs Supported	10,000				
Virtual CPUs (Minimum / Maximum)	1 / Unlimited				
Virtual Network Interfaces (Minimum / Maximum)	1 / 4				
Virtual Memory (Minimum / Maximum)	1GB / Unlimited				
Virtual Storage (Minimum)	40GB				
Device Quota	200GB	+200GB	+1TB	+8TB	+16TB
Sessions / Day	3.5 M	3.5 M	18 M	85 M	360 M

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 for both VMware ESX/ESXi and Microsoft Hyper-V Server virtualization environments.

VMware ESX/ESXi

- `.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.

Microsoft Hyper-V Server

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

Appendix B: FortiAnalyzer Log Limits

The following table outlines the device log limits and support information for FortiAnalyzer v5.0 Patch Release 3.

Table 14: FortiAnalyzer log limits

Model	Supported Devices / ADOMs / VDOMs / Log Arrays (Maximum)	GB / Day of Logs
FAZ-100C	150	5GB / Day
FAZ-200D	150	5GB / Day
FAZ-300D	175	15GB / Day
FAZ-400B	200	15GB / Day
FAZ-400C	200	15GB / Day
FAZ-1000B	2000	25GB / Day
FAZ-1000C	2000	25GB / Day
FAZ-1000D	2000	50GB / Day
FAZ-2000A	2000	75GB / Day
FAZ-2000B	2000	75GB / Day
FAZ-3000D	2000	250GB / Day
FAZ-4000A	2000	150GB / Day
FAZ-4000B	2000	Unlimited[a]
FAZ-VM-Base	10000	1GB / Day
FAZ-VM-GB1	10000	+1GB / Day
FAZ-VM-GB5	10000	+5GB / Day
FAZ-VM-GB25	10000	+25GB / Day
FAZ-VM-GB100	10000	+100GB / Day

a. Only restricted to the hardware performance, there are no software licensing limitations.

For more information including performance data (sessions/day, maximum log rate, average retention, and hardware specifications), see the FortiAnalyzer product datasheet available on the Fortinet web site, http://www.fortinet.com/products/fortianalyzer/index.html.