FortiAnalyzer v5.0 Patch Release 2
Release Notes

FortiAnalyzer v5.0 Patch Release 2 Release Notes

October 15, 2013

05-502-192378-20131015

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
2013-03-28	Initial release.
2013-04-12	Minor document update to Upgrade Information chapter.
2013-04-22	Added bug ID 0202921 to Known Issues chapter.
2013-05-10	Added FAZ-300D to supported models. Removed performance data from the appendix table. See the datasheet, http://www.fortinet.com/products/fortianalyzer/index.html for performance related information. Updated the Upgrade Information, Special Notices chapter and VM appendix.
2013-05-16	Corrected typographic issues.
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 2 build 0151.

Supported models

The following models are supported on FortiAnalyzer v5.0 Patch Release 2.

FortiAnalyzer

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

FAZ-300D

This model is released on a special branch based off of FortiAnalyzer v5.0 Patch Release 2. As such, the build number found in the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4018` 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 `0151`.

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 2:

- Log arrays

  Log arrays have been added to support group-based access to logs and reports. Log arrays are available in the *Device Manager* tab in the *Devices & Groups* menu. Log arrays also allow you to manage log data belonging to FortiGate HA clusters from a single device object. When adding new devices using the *Add Device* wizard, you can specify which log array to associate with the device or VDOM. You can configure RTM profiles and schedule reports for each log array. The maximum number of log arrays varies for each FortiAnalyzer model. See the *FortiAnalyzer v5.0 Patch Release 2 Administration Guide* for information on configuring log arrays.
- Group reports

  FortiAnalyzer v5.0 Patch Release 2 improves support for grouping devices/VDOMs for each report and displaying the generated report for each device.
- Log based alerts

You can configure log based alerts based on certain logging filters. You can select to send the alert to an email address, SNMP server, or syslog server. Alerts can be configured per device or per log array. The maximum number of alerts is 1000 for all FortiAnalyzer models.

- Backup/restore logs and reports
- CLI command branch change

  In FortiAnalyzer v5.0 Patch Release 2, the `fmsystem` and `fasystem` CLI branches have been merged into the `system` branch.
- Client reputation report template

  FortiOS logs being sent to FortiAnalyzer include a client reputation score that is used by FortiAnalyzer to calculate client reputation and generate a client reputation chart for *Top 10 Clients*.
- FortiClient logging to FortiAnalyzer

  Support has been added to FortiAnalyzer to allow you to log FortiClient endpoint traffic. In this release, FortiClient logs are able to be stored and downloaded from the *Log View* tab. In a future release, support will be added to view FortiClient devices in the *Device Manager*, view logs in *Log View*, and create reports based on FortiClient logs. For more information, see the *FortiClient v5.0 Patch Release 3 Administration Guide*.
- Pre-defined charts and datasets for wireless support
- Reliable FortiAnalyzer logging from FortiGate

  FortiAnalyzer v5.0 Patch Release 2 support reliable logging. The FortiGate can send logs to the FortiAnalyzer on port 514 TCP. For more information on configuring your FortiGate see the *CLI Reference for FortiOS 5.0*.
- Report template updates

  The following report templates have been added in FortiAnalyzer v5.0 Patch Release 2: Dial up VPN User report, SSL VPN User report, and Web Filter report.
- Import/export report templates
- SNMP support and MIB updates
- SQL query tool in the Web-based Manager

  An SQL query tool has been added to the Web-based Manager to allow you to test SQL datasets. After you choose a log type and set up variables for the filter you can test the SQL query before saving the setting.
- *RAID Monitor* widget enhancement
- *System Resources* widget enhancement
- XML web service support

  FortiAnalyzer web services has been enhanced to support SQL reporting. The following APIs are now supported in SQL: `runFazReport`, `getFazGeneratedReport`, `listFazGeneratedReports`, `getFazArchive`, `removeFazArchive`, `getSystemStatus`, `getFazConfig`, `setFazConfig`, and `searchFazLog`.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer v5.0 Patch Release 2 build 0151.

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.

Device groups

Device groups are not supported in FortiAnalyzer v5.0 Patch Release 2. 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 2 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.

ConnectWise Management Services Platform (MSP) support

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

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
```

Syslog device support

Syslog devices are not supported in FortiAnalyzer v5.0 Patch Release 1 or later. After upgrading your FortiAnalyzer, the syslog devices and logs cannot be displayed. The raw log files are stored in the device hard drives. Syslog device support will be added in a future release.

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.

FortiCache, FortiWeb, and FortiMail logging support

FortiAnalyzer v5.0 Patch Release 1 or later currently does not support FortiCache, FortiWeb, and FortiMail logging. Upon upgrading from v4.0 MR3 to v5.0 Patch Release 1 or later, only FortiOS and FortiOS Carrier are supported. Support for FortiCache, FortiWeb, and FortiMail will be added in a future release.

Upgrade Information

Upgrading from FortiAnalyzer v5.0 Patch Release 1

FortiAnalyzer v5.0 Patch Release 2 build 0151 officially supports upgrade from FortiAnalyzer v5.0 Patch Release 1.

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 2 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 2.

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` 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 6 or later to v5.0 Patch Release 2 is supported. The old VM license is converted into the new VM stackable license model. New VM installations running v5.0 Patch Release 2 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 2, 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 2 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
- Device groups
- 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.

General firmware upgrade steps

The following table lists the general firmware upgrade steps.

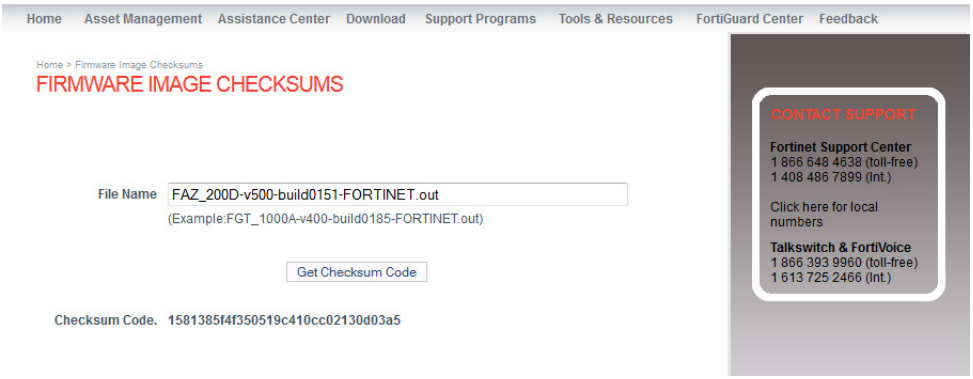
Table 1: Upgrade steps

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



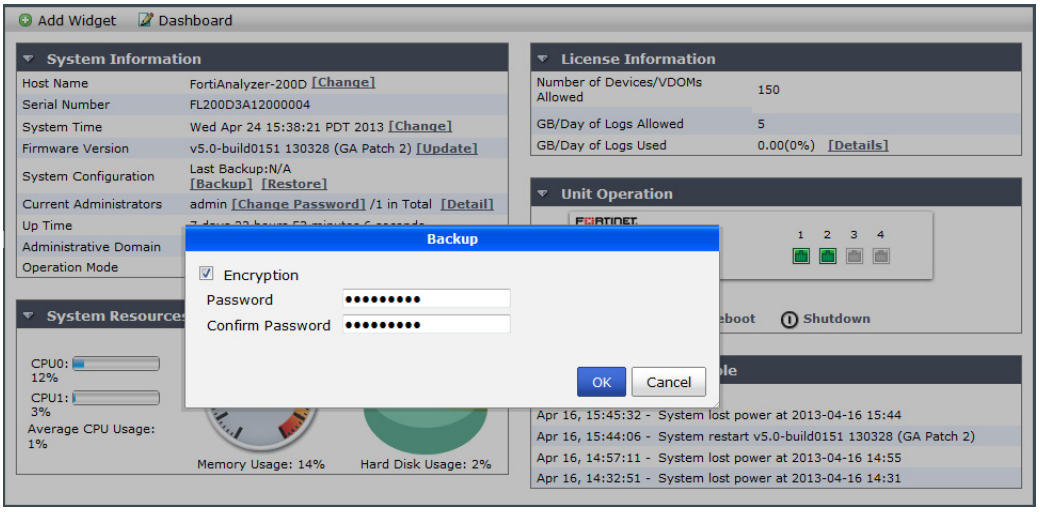
3. Enter the file name and select *Get Checksum Code* to get the firmware image checksum code. Compare this checksum with the checksum of the firmware image.

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

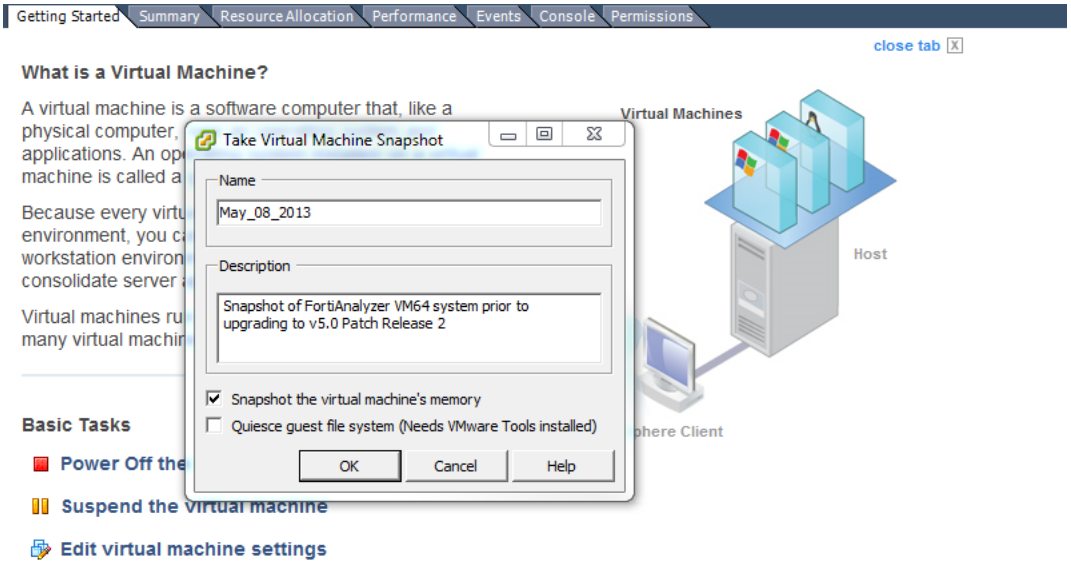


3. Select the checkbox to encrypt the backup file and enter a password.

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.
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

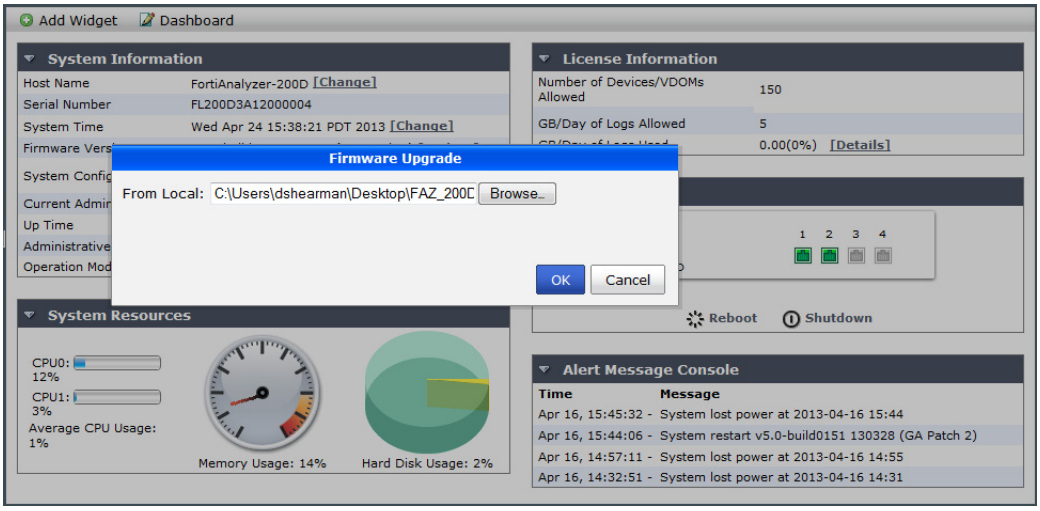


Step 3: Transfer the firmware image to your FortiAnalyzer device

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

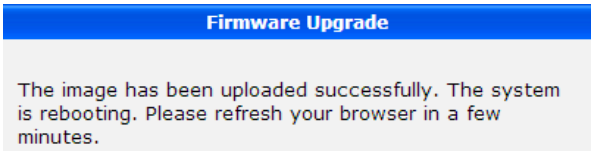
   The *Firmware Upgrade* dialog box opens.

Figure 4: Firmware upgrade dialog box



3. Select *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support web site 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



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
```

Product Integration and Support

Web browser support

FortiAnalyzer v5.0 Patch Release 2 supports the following web browsers:

- Microsoft Internet Explorer versions 8 and 9
- Mozilla Firefox version 24

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

FortiOS support

FortiAnalyzer v5.0 Patch Release 2 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 v4.0 MR2 is no longer supported (EOS) as of April 1, 2013.

FortiOS Carrier support

FortiAnalyzer v5.0 Patch Release 2 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

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

FortiMail support

FortiAnalyzer v5.0 Patch Release 2 does not support FortiMail logging. Support will be added in a future release.

FortiSwitch support

FortiAnalyzer v5.0 Patch Release 2 does not support FortiSwitch logging.

FortiClient support

FortiAnalyzer v5.0 Patch Release 2 supports the following FortiClient versions:

- FortiClient (Windows) v5.0 Patch Release 2
- FortiClient (Mac OS X) v5.0 Patch Release 2

MySQL Server support

FortiAnalyzer v5.0 Patch Release 2 supports MySQL Server version 5.5.

Virtualization software support

FortiAnalyzer v5.0 Patch Release 2 supports the following virtualization software:

- VMware ESX versions 4.1
- VMware ESXi versions 4.1 and 5.1

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 and FortiCarrier models and firmware versions can log to a FortiAnalyzer appliance running FortiAnalyzer v5.0 Patch Release 2. Please ensure that the devices that you manage are supported before completing the upgrade.

Table 3: 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-90D, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, 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-3600C, 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, FWF-90D FS-5203B	v5.0
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 4: Supported FortiCarrier models

Model	Firmware Version
FCR-3240C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5101C 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 2 build 0151. For inquires about a particular bug, please contact Customer Service & Support.

FortiAnalyzer VM

Table 5: Resolved FortiAnalyzer VM issues

Bug ID	Description
0191973	Failed to install a v5.0 FAZ-VM license file after upgrading from v4.0 MR3 Patch Release 6 to v5.0 Patch Release 1.

Logging

Table 6: Resolved logging issues

Bug ID	Description
0187182	The log date and time is shown incorrectly in the alert email log.
0189544, 0197200	*Log Browse* should support different download formats.
0194245	The `fortilogd` daemon stops receiving logs after a change is made to device level settings.
0198714	The GTP log field `deny_cause` does not appear in column settings in the Web-based Manager.

Reporting

Table 7: Resolved reporting issues

Bug ID	Description
0173417	FortiAnalyzer web services should support SQL reporting.
0177606	Reports show duplicate numbers in the *totalnum* column for any TopX reports when ranking is enabled.
0181606	The `fortilogd` daemon should apply the FortiGate's time zone setting before inserting the logs into the SQL database.
0186356	SQL reports will show duplicate entries when *hcache* is enabled.
0191113	Custom reports do not generate data.
0193889	The downloaded report name does not match the actual report name.

Table 7: Resolved reporting issues (continued)

Bug ID	Description
0194553	Unable to add the variable filters to a newly created dataset in the Web-based Manager.
0194905	FortiAnalyzer is unable to email scheduled reports.

System Settings

Table 8: Resolved system settings issues

Bug ID	Description
0163501	FortiAnalyzer CLI console sessions do not timeout.
0172303	NTPv3 with MD5 authentication does not work.
0188132	The default Web-based Manager disk label is incorrect for some FortiAnalyzer models.
0189543	A firmware downgrade from v5.0 Patch Release 1 to v4.0 MR3 results in an unrecoverable device state. The `FortiBootLoader` reports an `Open boot device failed` error message.
0193854	The `uploadd` daemon should preserve the file-system space.
0196575	The `set default-disk-quota` CLI command does not work.

Known Issues

The known issues tables listed below do not list every bug that has been identified with FortiAnalyzer v5.0 Patch Release 2 build 0151. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Logging

Table 9: Known logging issues

Bug ID	Description
0172792	A list of possible log fields should be added for the log search feature.
0193937	When two administrators are logged into FortiAnalyzer, the filters applied by admin 'A' will show up in the filter for admin 'B'.
0194012	Cannot display custom fields in *Log View*.
0195134	Displaying entries in log view is slower than anticipated.
0196813	When downloading a log in *raw log* or *Current view* and *CSV* is selected, FortiAnalyzer should change the name of the file to .csv format.
0197366	Cannot create a new syslog/SMTP/SNMP server from the alert trigger page.
0200952	The last page of the *Traffic Log* is blank.

Reporting

Table 10: Known reporting issues

Bug ID	Description
0172779	In SQL reports the week starts on Sunday. It is currently not possible to change the start date to Monday.
0189660	A previously configured report schedule failed after the device name was changed.
0194687	The `execute sql-report run` CLI command does not list the schedule names, instead the numerical position in the list is displayed.
0197325	Custom chart data typing is missing.
0197460	FortiAnalyzer v5.0 does not currently support French language reports.
0200514	Client reputation score filter issue. The greater than and less than logic in log view filters is currently not supported.

System Settings

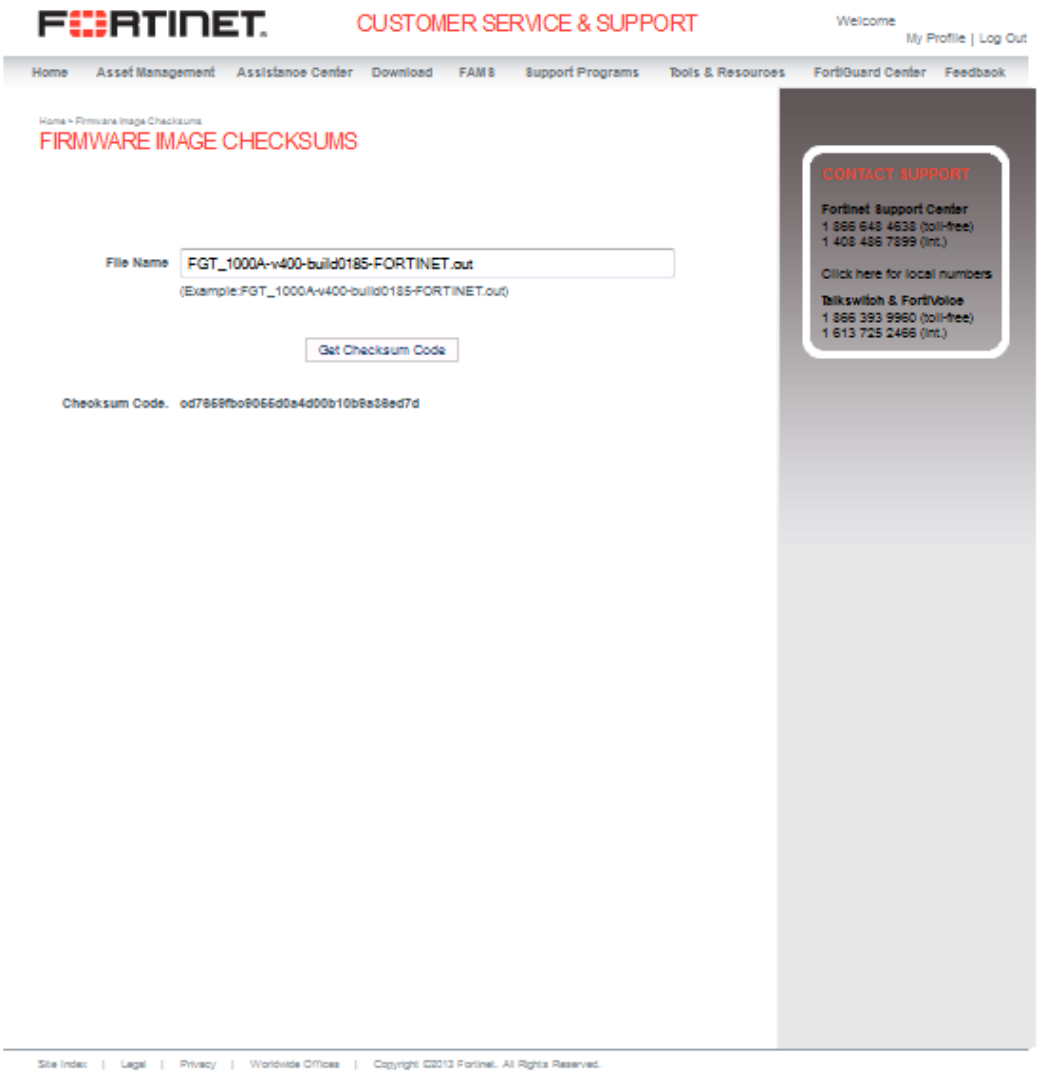
Table 11: Known system settings issues

Bug ID	Description
0189007	Received a *Web Server 500* error message when adding a device using the *Add Device* wizard.
0199778	The USB Modem dashboard widget does not display USB modem information.
0200401	The Device Manager log is incorrect when the VDOM has a long name.
0200596	The remote database cannot automatically rebuild after an upgrade.
0200834	The Device Manager log array quota always displays 0%.
0202921	When switching to collector mode without setting a remote IP, the FortiAnalyzer will randomly set the IP.

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 12 and consider future expansion.

Table 12: 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				
VM Form Factor	Open Virtualization Format (OVF)				
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

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

FortiAnalyzer VM licence enhancements

The following enhancements have been made to FortiAnalyzer VM:

- Stackable license model for FortiAnalyzer VM license add-ons
- License information is displayed on dashboard
- *Device Quota Storage* / *Device Quota Storage Used* displayed on dashboard

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.

Appendix B: FortiAnalyzer Log Limits

The following table outlines the device log limits and support information for FortiAnalyzer v5.0 Patch Release 2.

Table 13: 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-2000A	2000	75GB / Day
FAZ-2000B	2000	75GB / Day
FAZ-3000D	2000	150GB /Day
FAZ-4000A	2000	150GB / Day
FAZ-4000B	2000	150GB / Day
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

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.