FortiAnalyzer v5.0 Patch Release 6
Release Notes

FortiAnalyzer v5.0 Patch Release 6 Release Notes

September 08, 2015

05-506-225562-2015908

Fortinet Document Library	docs.fortinet.com
Fortinet Video Library	video.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
2014-02-05	Initial release.
2014-02-11	Added FG-1500D and FG-3700D to Table 4.
2014-02-12	Added FG-5001A and FG-VM64-AWS to Table 4.
2014-02-24	Updated Pre-processing logic of ebtime special notice to include explicit proxy log (logid=10) support.
2014-03-18	Updated upgrade information.
2014-03-19	Added FAZ-3000E to supported models.
2014-03-28	Added FAZ-3500E to supported models.
2014-04-15	Added FortiOS and FortiOS Carrier v5.0 Patch Release 7 support to Product Integration and Support.
2014-08-25	Added FortiOS and FortiOS Carrier v5.0 Patch Release 8 and 9 support to Product Integration and Support.
2015-08-10	Added Retain Device Information to Special Notices. Added Bug ID 236228 to Known Issues List.

Introduction

This document provides a summary of enhancements, support information, installation instructions, integration, resolved and known issues in FortiAnalyzer v5.0 Patch Release 6 build 0310. Please review all sections in this document prior to upgrading your device. For more information on upgrading your FortiAnalyzer device, see the *FortiAnalyzer Administration Guide*.

This document includes the following sections:

Supported models

The following models are supported on FortiAnalyzer v5.0 Patch Release 6.

FortiAnalyzer

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

FAZ-3000E

This model is released on a special branch based off of FortiAnalyzer v5.0 Patch Release 6. As such, the build number found in the *System* > *Dashboard* page and the output from the `get system status` CLI command displays `4047` as the build number.

FAZ-3500E

This model is released on a special branch based off of FortiAnalyzer v5.0 Patch Release 6. As such, the build number found in the *System* > *Dashboard* page and the output from the `get system status` CLI command displays `4031` as the build number.

FortiAnalyzer VM

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

See the Fortinet Document Library for FortiAnalyzer v5.0 documentation.

What's new in FortiAnalyzer v5.0 Patch Release 6

The following is a list of new features and enhancements in FortiAnalyzer v5.0 Patch Release 6 build 0310.

Charts

- Chart improvements

  Charts in the Chart Library are listed by alphabetical order by default. Charts have been renamed for improved usability. Improved chart library and database.
- New charts
  - Botnet activity charts

    Four new charts have been added for Botnet activity.
  - Site-to-Site VPN charts

Reports

- Report improvements
  - Bandwidth and Applications Report
  - Security Analysis report
  - Threat Report
  - User Report
  - Web Usage Report

Logging

- Improved FortiAnalyzer insert rate performance
- Log filter improvements
- When FortiAnalyzer is configured in Collector Mode, you can configure Log Forwarding in the Device Manager tab.

Other

- File Management

  Automatically delete log files, quarantined files, reports, and content archive files older than a specified time period.
- Event Management improvements

  FortiOS v4.0 MR3 logs are now supported in Event Management. Support subject customization of alert email.
- FortiAnalyzer VM supports up to 12 virtual disks (LVM)

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer v5.0 Patch Release 6 build 0310.

Retaining Devices after upgrading to FortiAnalyzer v5.0.6

Due to a known technical issue, devices may be lost after upgrading to FortiAnalyzer v5.0.6 from v4.3. If you wish to retain the devices and their logs, please contact technical support for assistance.

Event Management default settings

The default event handlers have been updated in FortiAnalyzer v5.0 Patch Release 6. After upgrade, the default status is *Disabled* and *All Devices* is selected. The filters used by the default event handlers have been updated.

Collector mode upgrade

After upgrading to FortiAnalyzer v5.0 Patch Release 6, the `sql status` is set to `disable` and the *Log View* tab is not available in the Web-based Manager. To enable the *Log View* tab and view logs, enter the following CLI commands:

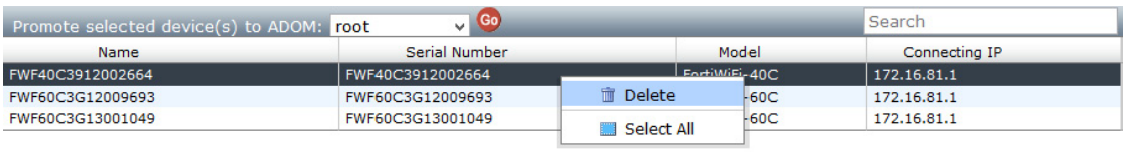
```
config system sql
  set status local
  end
```

Unregistered device table

In FortiAnalyzer v5.0 Patch Release 4 or earlier releases, the `config system global set unregister-pop-up` command is enabled by default. When a FortiGate device is configured to send logs to FortiAnalyzer, the unregistered device table will be displayed. You can decide to promote the device now or at a later date.

In FortiAnalyzer v5.0 Patch Release 5 or later, the `config system global set unregister-pop-up` command is disabled by default. When a FortiGate device is configured to send logs to FortiAnalyzer, the unregistered device table will not be displayed. Instead, a new entry *Unregistered Devices* will appear in the Device Manager tab under *All FortiGate*. You can then promote devices to specific ADOMs or use the right-click menu to delete the device.

Figure 1: Promote unregistered devices



SQL log table upgrade

When upgrading from FortiAnalyzer v4.0 MR3 Patch Release 7, v4.0 MR3 Patch Release 8, or v5.0 Patch Release 3 to v5.0 Patch Release 6, it is recommended to enable `auto-table-upgrade` before upgrading to avoid potential log view and reporting issues. To enable `auto-table-upgrade` enter the following CLI commands:

```
config system sql
  set auto-table-upgrade enable
end
```

After upgrading to v5.0 Patch Release 6, the SQL log table upgrade will start at the system start time. The SQL log table upgrade applies to both local SQL and MySQL databases.

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.

In FortiAnalyzer v5.0 Patch Release 5 or later, Explicit Proxy logs (`logid=10)` are checked when calculating the estimated browsing time.

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.

Upgrade to the latest VMware ESXi 4.1 Patch Release (build 800380 or later) before upgrading FortiAnalyzer VM or changing the vCPU setting. If ESXi server instability or a purple diagnostic screen issue persists, please contact VMware support for proper guidance.

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 6 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 5

FortiAnalyzer v5.0 Patch Release 6 build 0310 officially supports upgrade from FortiAnalyzer v5.0 Patch Release 5.

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 6 Administration Guide* available in the Fortinet Document Library.

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

FortiAnalyzer v5.0 Patch Release 6 build 0310 officially supports upgrade from FortiAnalyzer v4.0 MR3 Patch Release 7 or later.

Upon upgrading to FortiAnalyzer v5.0 Patch Release 5, 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.

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.

Upgrade to the latest VMware ESXi 4.1 Patch Release (build 800380 or later) before upgrading FortiAnalyzer VM or changing the vCPU setting. If ESXi server instability or a purple diagnostic screen issue persists, please contact VMware support for proper guidance.

Due to a known technical issue, devices may be lost after upgrading to FortiAnalyzer v5.0.6 from v4.3. If you wish to retain the devices and their logs, please contact technical support for assistance.

FortiAnalyzer VM license

Upgrading a FortiAnalyzer VM device from v4.0 MR3 Patch 6 or later to v5.0 Patch Release 6 is supported. The old VM license is converted into the new VM stackable license model. New VM installations running v5.0 Patch Release 6 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 6, 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 6 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

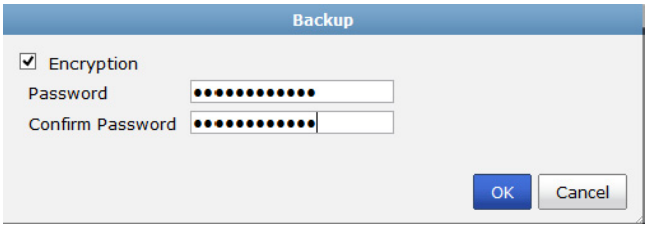
1. Make sure all log devices are running the supported firmware version as stated in the "Product Integration and Support" on page 19.
2. Download the firmware image from the Customer Service & Support portal.
3. Verify the integrity of the image using the *Firmware Image Checksums* tool. For more information, see "Firmware Image Checksums" on page 30.

Step 2: Back up your FortiAnalyzer configuration

1. Go to *System Settings* > *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 6 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 (VMware)

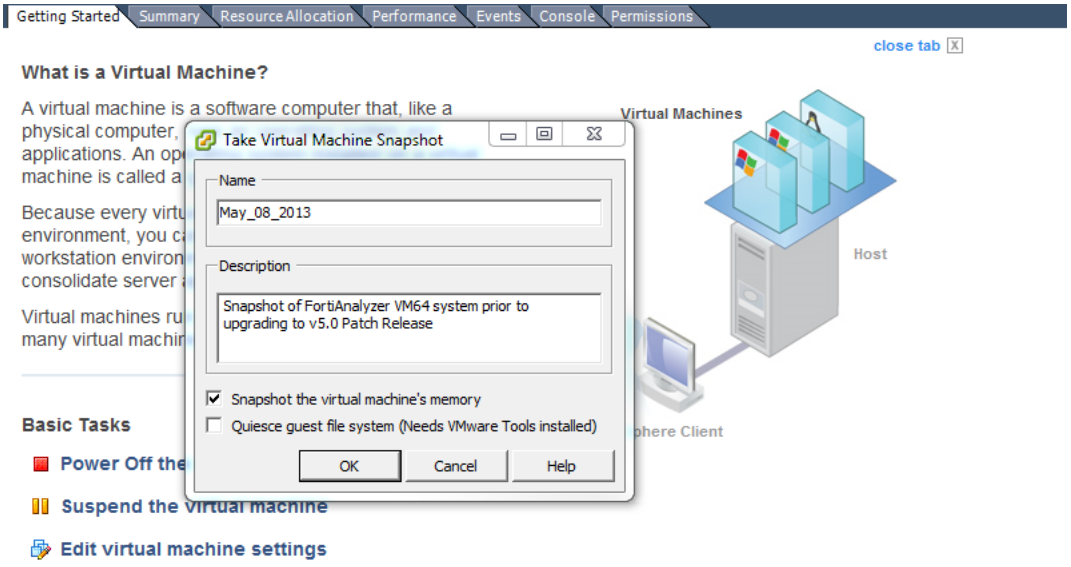
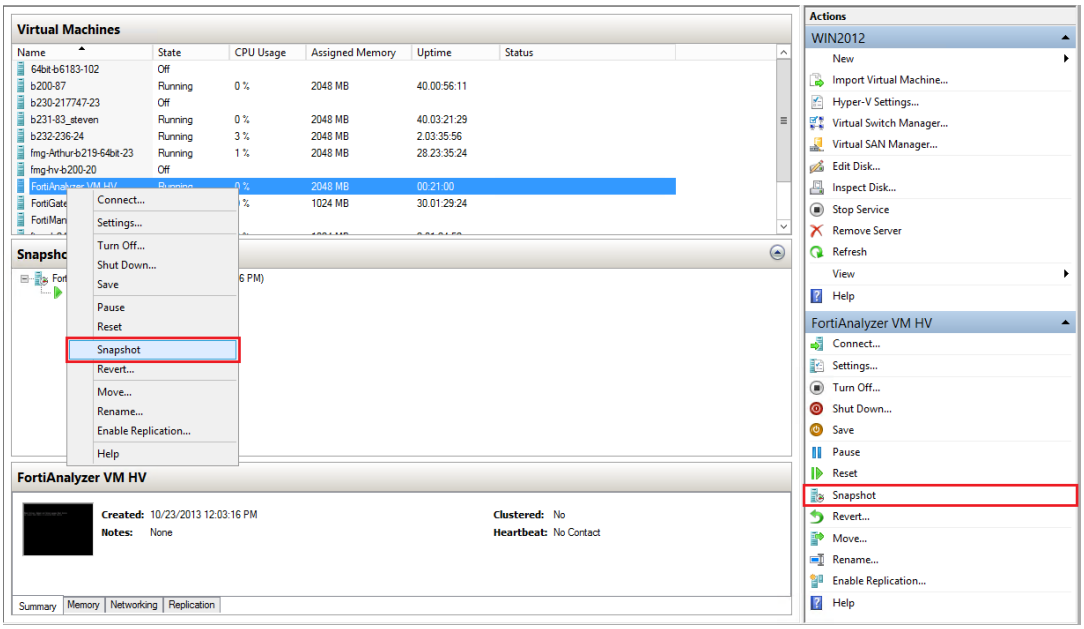


Figure 4: Snapshot of FortiAnalyzer VM (Microsoft Hyper-V)

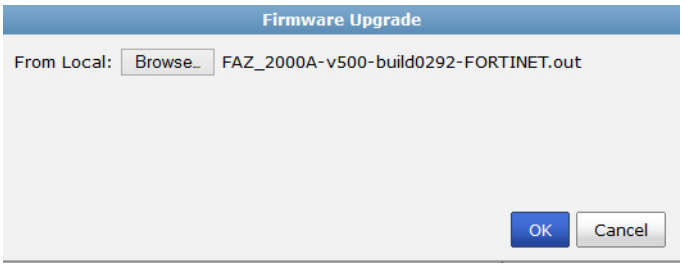


Step 3: Transfer the firmware image to your FortiAnalyzer device

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

   The *Firmware Upgrade* dialog box opens.

   Figure 5: Firmware upgrade dialog box



3. Select *Browse* to locate the firmware image (`.out` file) that you downloaded from the Fortinet Customer Service & Support portal and select *Open*.
4. Select *OK*. *Your* FortiAnalyzer will upload the firmware image and you will receive the following message: *The firmware upload is complete. The upgrade process has begun. Please refresh your browser in a few minutes*.

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 6 supports the following web browsers:

- Microsoft Internet Explorer versions 10 and 11
- Mozilla Firefox version 28
- Google Chrome version 34

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

FortiOS support

FortiAnalyzer v5.0 Patch Release 6 supports the following FortiOS versions:

- v5.0.0 and Patch Releases 1 to 9
- v4.0 MR3 Patch Release 2 to 15
- v4.0 MR2 and all Patch Releases

FortiOS Carrier support

FortiAnalyzer v5.0 Patch Release 6 supports the following FortiOS Carrier versions:

- v5.0.0 and Patch Releases 1 to 9
- v4.0 MR3 Patch Release 2 to 15
- v4.0 MR2 and all Patch Releases

FortiMail support

FortiAnalyzer v5.0 Patch Release 6 supports the following FortiMail versions:

- v5.0 MR1
- v5.0 Patch Release 3

FortiWeb support

FortiAnalyzer v5.0 Patch Release 6 supports the following FortiWeb versions:

- v5.0 MR1 Patch Release 1
- v5.0 Patch Release 5

FortiSwitch support

FortiAnalyzer v5.0 Patch Release 6 does not support FortiSwitch logging.

FortiClient support

FortiAnalyzer v5.0 Patch Release 6 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 6 supports MySQL Server v5.5.

Virtualization software support

FortiAnalyzer v5.0 Patch Release 6 supports the following virtualization software:

- VMware ESX version 4.1
- VMware ESXi versions 4.1, 5.1, and 5.5
- Microsoft Hyper-V Server 2008 R2 and 2012

Other virtualization software versions may function correctly, but are not supported by Fortinet. See "FortiAnalyzer VM" on page 31 for more information.

Feature support

The following table lists FortiAnalyzer feature support for log devices.

Table 2: Feature support per platform

Platform	Log View	Drill Down	Event Management	Reports
FortiGate	✔	✔	✔	✔
FortiCarrier	✔	✔	✔	✔
FortiMail	✔			✔
FortiWeb	✔			✔
FortiClient	✔			
FortiSwitch				

Language support

The following table lists FortiAnalyzer language support information.

Table 3: 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 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 6. Please ensure that the log devices are supported before completing the upgrade.

Table 4: Supported FortiGate models

Model	Firmware Version
FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60D, FG-60D-POE, FG-60D-3G4G-VZW, FG-80C, FG-80CM, FG-90D, FG-90D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-240D, FG-280D-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-1500D, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B, FG-5001A, FG-5001B, FG-5001C, FG-5101C FGR-100C FG-VM, FG-VM64, FG-VM-64-AWS, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE 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-VM, 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

Table 4: Supported FortiGate models (continued)

Model	Firmware Version
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 5: Supported FortiCarrier models

Model	Firmware Version
FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5101C	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 6: Supported FortiMail models

Model	Firmware Version
FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B FE-VM64	v5.0 MR1
FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B FE-VM64	v5.0 Patch Release 3

Table 7: Supported FortiWeb models

Model	Firmware Version
FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-4000D FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER	v5.0 MR1 Patch Release 1
FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-4000D FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER	v5.0 Patch Release 5

Resolved Issues

The resolved issues tables listed below do not list every bug that has been corrected with FortiAnalyzer v5.0 Patch Release 6 build 0310. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Drill Down

Table 8: Resolved drill down issues

Bug ID	Description
0224932	When SQL report is running and logs are being received at a high rate (6K logs per second), the Drill Down chart never loads and the page displays *Getting data .... 95%* for several minutes.

Event Management

Table 9: Resolved event management issues

Bug ID	Description
0225729	The event display column sorting is on a per-page basis rather than for all events.

Logging

Table 10: Resolved logging issues

Bug ID	Description
0202896	Added a pop-up dialog box to acknowledge that the log file import has completed.
0215991	Search does not work for some log fields in real-time mode.
0218853	FortiAnalyzer incorrectly logs ICMP traffic with destination port 2048.
0220901	Log backup fails halfway through the process and `newcli` process keeps running.
0221471	When logs are downloaded, FortiAnalyzer adds a line break after the date for NTP events.
0221695	Log search always auto fills entries when the current search matches a historical search.
0221696	When a search is added to the bookmarks, it is not immediately displayed.
0222769	Syslog messages sent from FortiGate or forwarded via FortiAnalyzer are different.

Table 10: Resolved logging issues (continued)

Bug ID	Description
0223983	FortiAnalyzer should delete logs and tables according to the `auto-delete` settings even if a device is part of a log array.
0225157	FortiAnalyzer should gray out the example filter syntax on the search input box.
0226031	When searching something in a dataset/chart, the search is removed after editing the dataset/chart.
0226306	Report calendar time is off by one hour.
0226493	FortiAnalyzer shows logs in multiple rows when explicit proxy is used.
0228187	FortiAnalyzer displays a Web Server Error500 when trying to open a DLP archive that contains Thai or Chinese characters in the filename.
0228189	IPv6 destination IP should be properly displayed.
0228982	`auto-delete` drops all devices active tables instead one.

Other

Table 11: Other resolved issues

Bug ID	Description
0223775	FortiCarrier devices are lost after upgrading from v4.0.

Reporting

Table 12: Resolved reporting issues

Bug ID	Description
0172779	Added an option to configure the first day of the week for reports.
0196442	FortiAnalyzer truncates the report's filter list.
0209445	The timer for mouse over dataset information toolbox is too short.
0216400	FortiAnalyzer should be able to control numbers of rows in primary and secondary columns separately.
0218429	Bar charts that use the full name of an IPS attack do not fit in a bar chart.
0218556	FortiAnalyzer should be able to produce a table ordered by time period and by volume/count.
0219348	FortiAnalyzer may generate incomplete data in reports.
0220418	When adding two 3D charts, they do not fit in a single page.
0220580	When uploading a report via FTP, the file name contains the report name twice.

Table 12: Resolved reporting issues (continued)

Bug ID	Description
0220903	LDAP group filter does not work for LDAP query.
0221526	There should be a default image for report templates.
0221536	Report does not contain the `.gif` image from image header section.
0222137	Changed the SQL table partition to hybrid mode; time-based for log array and size-based for device.
0223906	The Admin and System Events Report does not reflect time zone changes in FortiAnalyzer.
0224722	Users may not be able to set a filter in the service field via Microsoft Internet Explorer.
0224726	FortiAnalyzer cannot import reports from a v5.0 Patch Release 2 backup.
0225226	When creating or editing a simple report output profile, FortiAnalyzer may display a *500 INTERNAL SERVER ERROR*.
0225513	Report generation may never complete and `run_sql_rpt` crashes.
0226028	In a report, it is not possible to specify a subnet as a report filter.
0226112	Reports in an ADOM include all VDOMs when the target device is selected as *All FortiGates*.
0228351	General area charts in FortiAnalyzer reports lack details.
0228574	Not able to disable the report schedule. When schedule is disabled, it does not validate the change.

System Settings

Table 13: Resolved system settings issues

Bug ID	Description
0155013	Unable to connect to the Web-based Manager after a secure connection has been established.
0196770	The `diagnose fortilogd msgrate-device` CLI command displays incorrect results.
0224539	FortiAnalyzer's system time does not synchronize with NTP server.
0226383	The Logs/Data Received widget provides inaccurate readings for data received.

Known Issues

The known issues tables listed below do not list every bug that has been identified with FortiAnalyzer v5.0 Patch Release 6 build 0310. For inquires about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Device Manager

Table 14: Known device manager issues

Bug ID	Description
0229986	FortiAnalyzer may take some time to respond when promoting a device. Workaround: Please add the device(s) again if the timer expires.
0236228	Some registered devices may be lost after upgrading to v5.0.6.

Drill Down

Table 15: Known drill down issues

Bug ID	Description
0230605	Drill Down does not work for wildcard authenticated user via RADIUS.

Event Management

Table 16: Known event management issues

Bug ID	Description
0230911	User defined settings in the default event handlers are lost after upgrade.

Logging

Table 17: Known logging issues

Bug ID	Description
0227141	During log aggregation, the IP address for an HA cluster is modified.
0229751	When performing syslog forwarding, the device name should be the device name configured on Collector.
0230058	FortiAnalyzer may intermittently modify the attachment in emails when using output profile to mail generated reports.
231009	Users can only download logs from the current visible page without any filters applied.

Other

Table 18: Other known issues

Bug ID	Description
0229965	An invalid device's IP address is shown after upgrading FortiAnalyzer to v5.0 from v4.0 MR3.

Reporting

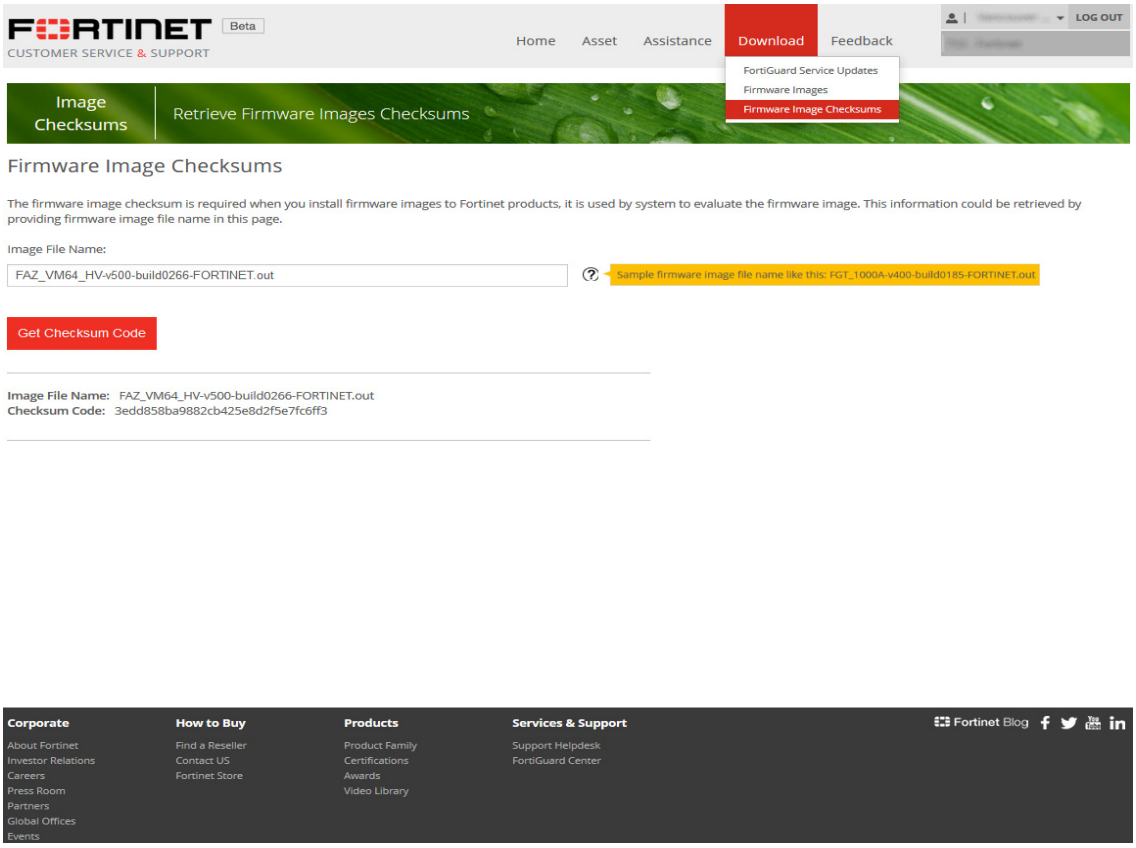
Table 19: Known reporting issues

Bug ID	Description
0228960	The table/chart will not output more than 1500 rows when generating a report.

Firmware Image Checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in, select *Download* > *Firmware Image Checksums*, enter the image file name 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 20 and consider future expansion.

Table 20: 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, 5.1, and 5.5 Microsoft Hyper-V Server 2008 R2 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)	2GB / Unlimited The default memory size is 2GB				
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 data sheet available in 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 firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the 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 6.

Table 21: 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	75GB / Day
FAZ-2000A	2000	75GB / Day
FAZ-2000B	2000	75GB / Day
FAZ-3000D	2000	250GB / Day
FAZ-3000E	2000	250GB / Day
FAZ-3500E	2000	Unlimited
FAZ-4000A	2000	150GB / Day
FAZ-4000B	2000	Unlimited
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 data sheet available on the Fortinet web site, http://www.fortinet.com/products/fortianalyzer/index.html.