



# FortiAnalyzer v5.2.0 Release Notes



## FortiAnalyzer v5.2.0 Release Notes

February 01, 2017

05-520-249463-20170201

Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet Document Library	<a href="https://docs.fortinet.com">docs.fortinet.com</a>
Fortinet Video Library	<a href="https://video.fortinet.com">video.fortinet.com</a>
Customer Service & Support	<a href="https://support.fortinet.com">support.fortinet.com</a>
Training Services	<a href="https://training.fortinet.com">training.fortinet.com</a>
FortiGuard	<a href="https://fortiguard.com">fortiguard.com</a>
Document Feedback	<a href="mailto:techdocs@fortinet.com">techdocs@fortinet.com</a>

# Table of Contents

<b>Change Log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
Supported models .....	5
What's new in FortiAnalyzer v5.2.0.....	6
<b>Special Notices</b> .....	<b>7</b>
Forward Compatibility with FortiOS 5.2.8 and Later .....	7
Limited support for remote SQL database .....	7
Changes to log aggregation .....	7
Upgrading from FortiAnalyzer v5.0.7 .....	7
Log Array relocation.....	7
Log Arrays, devices, and VDOMs.....	7
Generate reports during the database rebuild.....	8
Special characters in report name.....	8
Required changes to dataset.....	8
FortiAnalyzer VM.....	8
Pre-processing logic of ebtime.....	8
FortiAnalyzer VM license check.....	8
Extended UTM log for Application Control.....	9
ConnectWise Management Services Platform (MSP) support.....	9
Distributed upgrades .....	9
<b>Upgrade Information</b> .....	<b>10</b>
Upgrading from FortiAnalyzer v5.0.6 or later.....	10
Upgrading from FortiAnalyzer v5.0.5 or earlier.....	10
Downgrading to previous versions .....	10
Firmware image checksums .....	10
FortiAnalyzer VM firmware.....	11
SNMP MIB files.....	11
<b>Product Integration and Support</b> .....	<b>12</b>
FortiAnalyzer v5.2.0 support.....	12
Feature support .....	13
Language support.....	13
Supported models .....	14
<b>Resolved Issues</b> .....	<b>17</b>
<b>Known Issues</b> .....	<b>20</b>

# Change Log

Date	Change Description
2014-08-25	Initial release.
2014-09-04	Added the FAZ-2000B to the supported models list.
2014-09-09	Corrected FortiCache support information.
2014-11-13	Updated upgrade information.
2015-01-02	Added a special notice for changes to log aggregation.
2015-02-04	Added a special notice for changes to remote SQL database support.
2015-04-29	Updated VM Partition Information in the Upgrade Information chapter.
2015-06-02	Updated Upgrade Information Chapter.
2017-02-01	Updated to add a special notice about Forward Compatibility with FortiOS 5.2.8 and Later.

# Introduction

This document provides the following information for FortiAnalyzer v5.2.0 build 0618:

- Supported models
- What's new in FortiAnalyzer v5.2.0
- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues

For more information on upgrading your FortiAnalyzer device, see the [FortiAnalyzer Upgrade Guide](#).

## Supported models

FortiAnalyzer v5.2.0 supports the following models:

**Table 1:** Supported models

<b>FortiAnalyzer</b>	FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-1000C, FAZ-1000D, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, and FAZ-4000B.
<b>FortiAnalyzer VM</b>	FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.

## What's new in FortiAnalyzer v5.2.0

The following is a list of new features and enhancements in v5.2.0.

### Event Management

- Event Handler for local FortiAnalyzer event logs

### FortiView

- New FortiView module

### Logging

- Updated compact log v3 format from FortiGate
- Explicit proxy traffic logging support
- FortiSandbox support
- Syslog server support

### Reports

- Improvements to report configuration
- Improvements to the Admin and System Events Report template
- Improvements to the VPN Report template
- Improvements to the Wireless PCI Compliance Report template
- Improvements to the Security Analysis Report template
- New IPS Report template
- New Detailed Application Usage and Risk Report template
- New FortiMail Analysis Report template
- New pre-defined Application and Websites report templates
- Browsing Time report enhancement
- Macro library support
- Option to display or upload reports in HTML format
- FortiCache reporting support

### Other

- HA cluster auto discovery

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer v5.2.0.

## Forward Compatibility with FortiOS 5.2.8 and Later

Due to log field changes, FortiAnalyzer 5.2.0 is compatible with FortiOS/FortiOS Carrier 5.2.8 and later, but with possible interoperability issues. For full support, please upgrade to latest release of FortiAnalyzer.

## Limited support for remote SQL database

Starting with FortiAnalyzer software versions 5.0.7 and 5.2.0, remote SQL database support will only cover the insertion of log data into the remote MySQL database. Historical log search and reporting capabilities, which rely on the remote SQL data, will no longer be supported.

Those wishing to use the full set of FortiAnalyzer features are encouraged to switch as soon as possible to storing SQL data locally on the FortiAnalyzer. The local database can be built based upon existing raw logs already stored on the FortiAnalyzer.

## Changes to log aggregation

In FortiAnalyzer v5.2.0, new functionality was added to log aggregation to allow for multiple devices to be uploaded concurrently.

As a result, more information is included in the log aggregation negotiation messages. Both client and analyzer should be upgraded together to ensure log aggregation continues to work.

## Upgrading from FortiAnalyzer v5.0.7

When upgrading from v5.0.7 to v5.2.0, the FortiAnalyzer fails to automatically start rebuilding the database. You must manually start the rebuild process using the following CLI command, `execute sql-local rebuild-db`.

## Log Array relocation

*Log Array* has been relocated to *Log View* under the *FortiView* module from the *Device Manager* module.

## Log Arrays, devices, and VDOMs

In FortiAnalyzer v5.0.6 or earlier, when creating a Log Array with both devices and VDOMs, you need to select each device and VDOM to add it to the Log Array. In FortiAnalyzer v5.2.0 or later, when selecting to add a device with VDOMs, all VDOMs are automatically added to the Log Array.

## Generate reports during the database rebuild

After FortiAnalyzer is upgraded, the system may need to rebuild databases due to schema changes. Please note that the ability to generate accurate reports will be affected until the rebuild is complete.

## Special characters in report name

FortiAnalyzer v5.2 does not support the following special characters in report's name:

`\ / ' " > < & , |`

If you wish to import a report, please make sure the above special characters are not used. Otherwise, FortiAnalyzer may not display the name properly.

## Required changes to dataset

Due to database schema changes in FortiAnalyzer v5.2, the following rules must be followed by any existing or new datasets:

- If your dataset references any IP related data, such as `srcip` or `dstip`, please use the `ipstr('...')` function to convert an IP address for proper display. For example, `ipstr('srcip')` returns the source IP in a string.
- The column, `status`, has been changed to `action`. Please replace `status` with `action` in dataset query for proper status.

## FortiAnalyzer VM

In VM environments, upgrade your VM server to latest stable update and patch release offered by the VM host server provider before installing or upgrading FortiAnalyzer VM.

## 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 v5.0.5 or later, Explicit Proxy logs (`logid=10`) are checked when calculating the estimated browsing time.

## 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 v5.2.0, 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 in v5.2.

## Distributed upgrades

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



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

---

# Upgrade Information

## Upgrading from FortiAnalyzer v5.0.6 or later

FortiAnalyzer v5.2.0 supports upgrade from v5.06 or later.

FortiAnalyzer version 5.0.7 or later has re-sized the flash partition storing system firmware. If your FortiAnalyzer is running 5.0.6, you will need to change the hard disk provisioned size to more than 512 MB in your VM environment before powering on the FortiAnalyzer VM. The secondary firmware and System Settings stored in the partition is lost after upgrade. Please reconfigure System Settings as needed.

## Upgrading from FortiAnalyzer v5.0.5 or earlier

In order to accommodate the re-sizing of the flash partition, you **MUST** upgrade to v5.0.6 first.



Please upgrade your FAZ-100C via the Web-based Manager or command line interface. Upgrade via TFTP from BIOS is not supported for this model.

---

## Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous firmware release via the Web-based Manager or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

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

## 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>. To verify the integrity of the download, select the *Checksum* link next to the *HTTPS* download link. A dialog box will be displayed with the image file name and checksum code. Compare this checksum with the checksum of the firmware image.

## FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer VM firmware images for both VMware ESX/ESXi and Microsoft Hyper-V Server virtualization environments.

### 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.

### 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.

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

## SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiAnalyzer v5.00 file folder.

# Product Integration and Support

## FortiAnalyzer v5.2.0 support

The following table lists FortiAnalyzer v5.2.0 product integration and support information.

**Table 2:** FortiAnalyzer v5.2.0 support

<b>Web browser</b>	<ul style="list-style-type: none"><li>• Microsoft Internet Explorer versions 10 and 11</li><li>• Mozilla Firefox versions 30 and 31</li><li>• Google Chrome version 37</li></ul> <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
<b>FortiOS/FortiOS Carrier</b>	<ul style="list-style-type: none"><li>• v5.2.0–5.2.7 See “<a href="#">Forward Compatibility with FortiOS 5.2.8 and Later</a>” on page 7.</li><li>• v5.0.0 and later</li><li>• v4.3.2 and later</li></ul>
<b>FortiMail</b>	<ul style="list-style-type: none"><li>• v5.1.3</li><li>• v5.0.6</li></ul>
<b>FortiWeb</b>	<ul style="list-style-type: none"><li>• v5.2.1</li><li>• v5.1.4</li><li>• v5.0.6</li></ul>
<b>FortiCache</b>	<ul style="list-style-type: none"><li>• v3.0.0</li></ul>
<b>FortiClient</b>	<ul style="list-style-type: none"><li>• v5.2.0 and later</li><li>• v5.0.4 and later</li></ul>
<b>FortiSandbox</b>	<ul style="list-style-type: none"><li>• v1.4.0 and later</li></ul>
<b>Virtualization software</b>	<ul style="list-style-type: none"><li>• VMware ESX version 4.1</li><li>• VMware ESXi versions 4.1, 5.1, and 5.5</li><li>• Microsoft Hyper-V Server 2008 R2 and 2012</li></ul>

## Feature support

The following table lists FortiAnalyzer feature support for log devices.

**Table 3:** Feature support per platform

Platform	Logging	FortiView	Event Management	Reports
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiMail	✓			✓
FortiWeb	✓			✓
FortiCache	✓			✓
FortiClient	✓			
FortiSandbox	✓			
Syslog	✓			

## Language support

The following table lists language support information.

**Table 4:** Language support

Language	Web-based Manager	Reports	Documentation
English	✓	✓	✓
French		✓	
Spanish		✓	
Portuguese		✓	
Korean	✓	✓	
Chinese (Simplified)	✓	✓	
Chinese (Traditional)	✓	✓	
Japanese	✓	✓	
Russian		✓	
Hebrew		✓	
Hungarian		✓	

To change the 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*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can import language translation files for these languages via the command line interface using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP
address> <user name> <password> <file name>
execute sql-report import-lang <language name> <sftp> <server IP
address> <user name> <password> <file name>
execute sql-report import-lang <language name> <scp> <server IP
address> <user name> <password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP
address> <file name>
```

For more information, see the [FortiAnalyzer CLI Reference](#).

## Supported models

The following tables list which FortiGate, FortiCarrier, FortiMail, FortiWeb, FortiCache, and FortiSandbox models and firmware versions can log to a FortiAnalyzer appliance running v5.2.0. Please ensure that the log devices are supported before completing the upgrade.

**Table 5:** Supported FortiGate models

Model	Firmware Version
FG-20C, FG-20C-LENC, FWF-20C, FG-20C-ADSL-A, FWF-20C-ADSL-A, FG-30D, FWF-30D, FG-30D-POE, FWF-30D-POE, FG-40C, FG-40C-LENC, FWF-40C, FG-60C, FG-60C-LENC, FWF-60C, FG-60C-POE, FG-60C-SFP, FWF-60CM, FWF-60CX-ADSL-A, FG-60D, FWF-60D, FG-60D-POE, FWF-60D-POE, FG-80C, FG-80C-LENC, FG-80C-DC, FG-80CM, FWF-80CM, FWF-81CM, FG-90D, FWF-90D, FG-90D-POE, FWF-90D-POE, FG-100D, FG-100D-LENC, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-LENC, FG-200B-POE, FG-200D, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300C-LENC, FG-300C-DC, FG-310B, FG-310B-DC, FG-310B-LENC, FG-311B, FG-600C, FG-600C-DC, FG-600C-LENC, FG-620B, FG-620B-DC, FG-621B, FG-621B-DC, FG-800C, FG-800C-DC, FG-1000C, FG-1000C-DC, FG-1000C-LENC, FG-1240B, FG-1240B-DC, FG-1240B-LENC, FG-3016B, FG-3040B, FG-3040B-DC, FG-3040B-LENC, FG-3140B, FG-3140B-DC, FG-3140B-LENC, FG-3240C, FG-3240C-DC, FG-3600C, FG-3600DC, FG-3810A, FG-3810A-DC-FG-3810A-LENC, FG-3950B, FG-3950B-DC, FG-3950B-LENC, FG-3951B, FG-3951B-DC, FG-5001A, FG-5001B, FG-5001C, FG-5101C  FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN  FS-5203B	v5.2

**Table 5:** Supported FortiGate models (continued)

Model	Firmware Version
<p>FG-20C, FG-20C-LENC, FWF-20C, FG-20C-ADSL-A, FWF-20C-ADSL-A, FG-30D, FWF-30D, FG-30D-POE, FWF-30D-POE, FG-40C, FG-40C-LENC, FWF-40C, FG-60C, FG-60C-LENC, FWF-60C, FG-60C-POE, FG-60C-SFP, FWF-60CM, FWF-60CM-3G4G-B, FWF-60CX-ADSL-A, FG-60D, FWF-60D, FG-60D-3G4G-VZW, FG-60D-POE, FWF-60D-POE, FG-70D, FG-80C, FG-80C-LENC, FG-80C-DC, FG-80CM, FWF-80CM, FWF-81CM, FG-80D, FG-90D, FWF-90D, FG-90D-POE, FWF-90D-POE, FG-92D, FG-94D-POE, FG-100D, FG-100D-LENC, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-LENC, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-240D-POE, FG-280D-POE, FG-300C, FG-300C-LENC, FG-300C-DC, FG-300D, FG-310B, FG-310B-DC, FG-310B-LENC, FG-311B, FG-500D, FG-600C, FG-600C-DC, FG-600C-LENC, FG-620B, FG-620B-DC, FG-621B, FG-621B-DC, FG-800C, FG-800C-DC, FG-1000C, FG-1000C-DC, FG-1000C-LENC, FG-1240B, FG-1240B-DC, FG-1240B-LENC, FG-1500D, FG-3016B, FG-3040B, FG-3040B-DC, FG-3040B-LENC, FG-3140B, FG-3140B-DC, FG-3140B-LENC, FG-3240C, FG-3240C-DC, FG-3600C, FG-3600DC, FG-3700D, FG-3810A, FG-3810A-DC-FG-3810A-LENC, FG-3950B, FG-3950B-DC, FG-3950B-LENC, FG-3951B, FG-3951B-DC, FG-5001A, FG-5001B, FG-5001C, FG-5001D, FG-5101C</p> <p>FGR-60D, FGR-100C</p> <p>FGV-70D4</p> <p>FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN</p> <p>FS-5203B</p>	v5.0
<p>FG-20C, FG-20C-LENC, FWF-20C, FG-20C-ADSL-A, FWF-20C-ADSL-A, FG-30B, FWF-30B, FG-40C, FG-40C-LENC, FWF-40C, FG-50B, FG-50B-LENC, FWF-50B, FG-51B, FG-51B-LENC, FG-60B, FWF-60B, FG-60C, FG-60C-LENC, FWF-60C, FG-60C-POE, FG-60C-SFP, FWF-60CM, FWF-60CM-3G4G-B, FWF-60CX-ADSL-A, FG-80C, FG-80C-LENC, FG-80C-DC, FG-80CM, FWF-80CM, FWF-81CM, FG-82C, FG-100A, FG-100D, FG-100D-LENC, FG-110C, FG-111C, FG-200A, FG-200B, FG-200B-LENC, FG-200B-POE, FG-224B, FG-300A, FG-300C, FG-300C-LENC, FG-300C-DC, FG-310B, FG-310B-DC, FG-310B-LENC, FG-311B, FG-400A, FG-500A, FG-600C, FG-600C-DC, FG-600C-LENC, FG-620B, FG-620B-DC, FG-621B, FG-621B-DC, FG-800, FG-800C, FG-800C-DC, FG-800F, FG-1000, FG-1000A, FG-1000AFA2, FG-1000C, FG-1000C-DC, FG-1000C-LENC, FG-1240B, FG-1240B-DC, FG-1240B-LENC, FG-3016B, FG-3040B, FG-3040B-DC, FG-3040B-LENC, FG-3140B, FG-3140B-DC, FG-3140B-LENC, FG-3240C, FG-3240C-DC, FG-3600, FG-3600A, FG-3810A, FG-3810A-DC-FG-3810A-LENC, FG-3950B, FG-3950B-DC, FG-3950B-LENC, FG-3951B, FG-3951B-DC, FG-5001, FG-5001A, FG-5001B, FG-5001C, FG-5001FA2, FG-5001FA2-LENC, FG-5002A, FG-5002A-LENC, FG-5002FB2, FG-5005FA2, FG-5101C</p> <p>FGR-100C</p> <p>FG-ONE</p> <p>FG-VM, FG-VM64, FG-VM64-XEN</p> <p>FS-5203B</p>	v4.3

**Table 6:** Supported FortiCarrier models

Model	Firmware Version
FCR-3240C, FCR-3240C-DC, FCR-3600C, FCR-3600C-DC, FCR-3810A, FCR-3810A-DC, FCR-3950B, FCR-3950B-DC, FCR-3951B, FCR-3910B-DC, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5101C	v5.2
FCR-3240C, FCR-3240C-DC, FCR-3600C, FCR-3600C-DC, FCR-3810A, FCR-3810A-DC, FCR-3950B, FCR-3950B-DC, FCR-3951B, FCR-3910B-DC, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5101C	v5.0
FCR-3810A, FCR-3810A-DC, FCR-3950B, FCR-3950B-DC, FCR-3951B, FCR-3910B-DC, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2	v4.3

**Table 7:** 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	v5.1.3
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	v5.0.6

**Table 8:** 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	v5.0.6, v5.1.4, v5.2.1

**Table 9:** Supported FortiCache models

Model	Firmware Version
FCH-400C, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D FCH-VM64	v3.0.0

**Table 10:**Supported FortiSandbox models

Model	Firmware Version
FSA-1000D, FSA-3000D	v1.4.0, v1.4.1, v1.4.2

# Resolved Issues

The following issues have been fixed in FortiAnalyzer v5.2.0. For inquiries about a particular bug, please contact [Customer Service & Support](#).

## Device Manager

**Table 11:** Resolved device manager issues

Bug ID	Description
0213019	FortiOS Carrier version 4.3 and version 5.0 devices are recognized as FortiGate in the FortiAnalyzer unregistered device popup table.
0236228	Some registered device are lost after upgrading to version 5.0.6.
0246232	The FortiAnalyzer fails to load the Web-based Manager page when a name is used instead of an IP address.
0247125	A FortiCarrier device cannot be added into the unregistered table.

## Event Management

**Table 12:** Resolved event management issues

Bug ID	Description
0245374	Alert emails are not going through mailbox when using an authenticated SMTP server.
0247478	After upgrading the FortiAnalyzer, the Event Management is no longer able to send email messages.

## Logging

**Table 13:** Resolved logging issues

Bug ID	Description
0222140	<i>Log Browse</i> may take a long time to load logs.
0228960	FortiAnalyzer cannot generate a report with a chart that has more than 1500 rows.
0241572	FortiAnalyzer should be able to search logs by the FortiGate's hostname.
0245990	The FortiAnalyzer fails to insert a log message if it is missing a quotation mark character.
0246354	FortiView and Log View should consistently display IP addresses in quotations.
0248159	Log Browse's header and footer are lost when the window is scrolled.

**Table 13:** Resolved logging issues (continued)

Bug ID	Description
0248273	The FortiView source panel should support filtering by user.
0249053	Log arrays may not be displayed after upgrading from version 5.0.6.
0249963	Inconsistent fields are used in IPS historical and real-time views.

## Other

**Table 14:** Other resolved issues

Bug ID	Description
0151410	The FortiAnalyzer tunnel or SSL does not work when SHA256 is set or SSL encryption is set to high.
0213916	Help for the <code>sql-query-dataset</code> CLI command displays incorrect information.
0237989	Added an option to allow imported certificates to be used by OFTP to receive logs.
0241161	RAID-50 has smaller array space than is expected.
0244410	Patched SSL/TLS MITM vulnerability (CVE-2014-0224).

## Reporting

**Table 15:** Resolved reporting issues

Bug ID	Description
0167549	PDF reports with Russian, Hebrew, or Hungarian text are not readable.
0216211	The <code>dlpextra</code> field is missing in chart filters.
0218622	FortiAnalyzer does not generate reports based on global font settings set at the section level and at the layout level.
0224745	Portuguese language is displayed incorrectly in the Application and Risk Analysis report.
0232919	In a FortiMail ADOM, FortiAnalyzer should show <i>All FortiMails</i> as device instead of <i>All FortiGates</i> .
0233112	Use chart description instead of chart name when in generating a report.
0233234	FortiMail reports are not generated at the scheduled time.
0233861	Schedule report does not run if the ADOM name contains a space character.
0234007	The <code>Estimated-Browsing-Time</code> dataset fetches data for more than 24 hours instead of the time specified.
0235680	FortiAnalyzer has no advanced graphic chart when cloning the <i>Bandwidth Summary for Past 7 Days</i> chart.

**Table 15:** Resolved reporting issues (continued)

Bug ID	Description
0236004	After upgrade, all custom reports and output profiles are missing.
0237165	When importing a report with a chart name greater than 64 and less 128 characters, the chart name gets truncated to 64 characters and it cannot be found in the chart library.
0239770	Added a new pre-defined chart and dataset for OS type count.
0240971	Report advanced filters should ignore special characters.
0241927	There may a delay to display the progress of a report generation.
0242027	Predefined charts are duplicated after importing a report with predefined charts.
0242382	FortiAnalyzer shows an incorrect bar chart value for maximum CPU usage.
0242481	Reports do not show all devices when the <i>Print Device List</i> option is set as <i>Detailed</i> .
0243494	FortiAnalyzer needs to support query when entries are longer than 2048 characters.
0243699	System is shown as out of memory when generating a report.
0243853	When uploading a report to a FTP, SFTP, or SCP server, the report name and .zip file name should be as same as FortiAnalyzer report name.
0245933	When a big report is running for a long time, it generates a report with no data.
0247673	Report is lost after upgrade if report has IP filter configured.
0247935	When generating a report for FortiMail, all virus charts always report with positive entries.

## System Settings

**Table 16:** Resolved system settings issues

Bug ID	Description
0231733	Log aggregation does not forward all logs from the previous day.

# Known Issues

The following issues have been identified in FortiAnalyzer v5.2.0. For inquires about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

## Event Management

**Table 17:** Known event management issues

Bug ID	Description
0249212	Event handler cannot match multiple filters specified for text filter.
0251790	Event cannot be triggered after changing the ADOM name. Workaround: To remedy the issue, please run the <code>diagnose test application sqllogd 200 reload</code> CLI command.
0251797	Event cannot be triggered after adding a new device to a log array. Workaround: To remedy the issue, please run the <code>diagnose test application sqllogd 200 reload</code> CLI command.

## Logging

**Table 18:** Known logging issues

Bug ID	Description
0247857	Log View replaces two spaces in message field with only one space.
0248384	Incorrect date for traffic logs and alerts delivery delay to RSA Envision syslog server.

## Other

**Table 19:** Other known issues

Bug ID	Description
0248969	FortiGate receives incorrect disk space information when testing FortiAnalyzer connectivity.

## Reporting

**Table 20:** Known reporting issues

Bug ID	Description
0247042	FortiAnalyzer generates a different result for cloned chart, <i>Virus Time Line</i> .

**Table 20:** Known reporting issues (continued)

Bug ID	Description
0250561	Users are unable to receive the event handler's email from FortiAnalyzer when the event handler is triggered.
0250679	After upgrade, FortiAnalyzer may not be able to generate reports due to missing default datasets.

## System Settings

**Table 21:** Known system settings issues

Bug ID	Description
0249199	The SNMP trap for low memory is sent when before the threshold is reached.

## Upgrade

**Table 22:** Known upgrade issues

Bug ID	Description
0252065	When upgrading from version 5.0.7 to version 5.2.0, the FortiAnalyzer fails to automatically start rebuilding the database. You must manually start the rebuild process using the following CLI command, <code>execute sql-local rebuild-db</code> .

