FERTINET.

FortiAnalyzer v5.0.9
Release Notes

FortiAnalyzer v5.0.9 Release Notes

April 29, 2015

05-508-257570-20150429

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
2014-10-23	Initial release.
2014-12-19	Added FAZ-VM64-AWS to supported models.
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.
2015-02-13	Updated the upgrade information section.
2015-04-29	Updated the VM Partition Information in the Upgrade Information chapter.

Introduction

This document provides the following information for FortiAnalyzer v5.0.9:

- Supported models
- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues

Please review all sections in this document prior to upgrading your device. For more information on upgrading your device, see the *FortiAnalyzer Upgrade Guide*.

Supported models

FortiAnalyzer v5.0.9 supports the following models:

Table 1: Supported models

FortiAnalyzer	FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-4000A, FAZ-4000B	Build 0342
FortiAnalyzer VM	FAZ-VM32, FAZ-VM64, FAZ-VM64-HV	Build 0342
FortiAnalyzer VM	FAZ-VM64-AWS	Build 4058
FortiAnalyzer VM	FAZ-VM64-KVM, FAZ-VM64-XEN	Build 4061

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer v5.0.9.

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 v5.0.9, 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.

Amazon Web Services

FortiAnalyzer v5.0.9 introduces a new 64-bit Amazon Machine Image (AMI).

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 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 v5.0.7 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 your device 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 v5.0.7 and later 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, your device may not display the name properly.

Required changes to dataset

Due to database schema changes in v5.0.7, 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.

Unregistered device table

In FortiAnalyzer v5.0.4 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 v5.0.5 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.

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 address with the IP information in the license file. If the IP address does 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 v5.0.9, 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 FortiAnalyzer v5.0.

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 version 5.0.6 or later

FortiAnalyzer v5.0.9 supports upgrade from v5.0.6 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 your FAZ-400B to v5.0.9 requires you to use an interim step. You MUST upgrade to v5.0.7 before upgrading to v5.0.9. For more information see the *FortiAnalyzer v5.0.7 Release Notes*. The upgrade path looks like this:
>
> *v5.0.5 or earlier >v5.0.6 > v5.0.7 > v5.0.9*

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, FAZ-2000A, or FAZ-4000A via the Web-based Manager or command line interface. Upgrade via TFTP from BIOS is not supported for these models.

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}
```

FortiAnalyzer VM firmware

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

Amazon Web Services
- The 64-bit Amazon Machine Image (AMI) is available in the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.

- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the QCOW2 file for Open Source XenServer.

- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.

- `.out.kvm.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains QCOW2 that can be used by qemu.

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.

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.

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 v5.0.9 support

The following table lists FortiAnalyzer v5.0.9 product integration and support information.

Table 2: FortiAnalyzer v5.0.9 support

Web Browsers	• Microsoft Internet Explorer versions 10 and 11 • Mozilla Firefox versions 32 and 33 • Google Chrome version 38 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• v5.2.0 and later • v5.0.0 and later • v4.3.2 and later • v4.2.0 and later
FortiMail	• v5.2.0 • v5.1.3 • v5.0.6
FortiWeb	• v5.3.0 • v5.2.3 • v5.1.4 • v5.0.6
FortiCache	• v3.0.0 and v3.0.1
FortiClient	• v5.2.0 and later • v5.0.4 and later
FortiSandbox	• v1.4.0, v1.4.1, and v1.4.2
Virtualization Environments	
Amazon	• Amazon Web Services AMI Amazon EC2, Amazon EBS
Citrix	• XenServer version 6.2
Linux KVM	• RedHat 6.5
Microsoft	• Hyper-V Server 2008 R2 and 2012

Table 2: FortiAnalyzer v5.0.9 support (continued)

Open Source	• XenServer version 4.2.5
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, and 5.5

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	✔	✔	✔	✔
FortiCache	✔			✔
FortiCarrier	✔	✔	✔	✔
FortiClient	✔			
FortiMail	✔			✔
FortiSandbox	✔			
FortiWeb	✔			✔
Syslog	✔			

Language support

The following table lists FortiAnalyzer language support information.

Table 4: Language support

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

Table 4: Language support (continued)

Language	Web-based Manager	Reports	Documentation
Russian		✔	
Spanish		✔	

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*.

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, FortiCache, FortiSandbox, and FortiWeb models and firmware versions can log to a FortiAnalyzer appliance running v5.0.9. Please ensure that the log devices are supported before completing the upgrade.

Table 5: Supported FortiGate models

Model	Firmware Version
FortiGate	v5.2
FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-POE, FG-70D, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-94D-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-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-800C, FG-1000C, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600C, FG-3810A, FG-3950B, FG-3951B, FG-5001A, FG-5001B, FG-5001C, FG-5101C	
FortiGate DC	
FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3240C-DC, FG-3600C-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC	
FortiGate Low Encryption	
FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-310B-LENC, FG-600C-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC	
FortiWiFi	
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,	
FortiGate VM	
FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN	
FortiSwitch	
FS-5203B	

Table 5: Supported FortiGate models (continued)

Model	Firmware Version
FortiGate	v5.0
FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-500D, FG-600C, FG-620B, FG-621B, FG-800C, FG-1000C, FG-1000D, FG-1200D, 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, FG-5001D	
FortiGate DC	
FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3240C-DC, FG-3600C-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC	
FortiGate Low Encryption	
FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC	
FortiWiFi	
FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CM-3G4G-B, FWF-60CX-ADSL-A, FWF-60D-POE, FWF-60D, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D	
FortiGate Rugged	
FGR-60D, FGR-100C	
FortiGateVoice	
FGV-70D4	
FortiGate VM	
FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN	
FortiSwitch	
FS-5203B	

Table 5: Supported FortiGate models (continued)

Model	Firmware Version
FortiGate	v4.3
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-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-311B, FG-400A, FG-500A, FG-600C, FG-620B, FG-621B, FG-800, FG-800C, FG-800F, FG-1000, FG-1000A, FG-1000AFA2, 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-5002A, FG-5002FB2, FG-5005FA2, FG-5101C	
FortiGate DC	
FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-620B-DC, FG-600C-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3240C-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC	
FortiGate Low Encryption	
FG-20C-LENC, FG-40C-LENC, FG-50B-LENC, FG-51B-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC, FG-5001FA2-LENC, FG-5002A-LENC	
FortiWiFi	
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	
FortiGate Rugged	
FGR-100C	
FortiGate One	
FG-ONE	
FortiGate VM	
FG-VM, FG-VM64, FG-VM64-XEN	
FortiSwitch	
FS-5203B	

Table 5: Supported FortiGate models (continued)

Model	Firmware Version
FortiGate FG-30B, FG-50B, FG-51B, FG-60B, FG-80C, FG-80CM, FG-80CM, FG-82C, FG-100A, FG-110C, FG-111C, FG-200A, FG-200B, FG-200B-POE, FG-224B, FG-300A, FG-300C, FG-310B, FG-311B, FG-400A, FG-500A, FG-620B, FG-621B, FG-800, FG-800F, FG-1000, FG-1000A, FG-1000AFA2, FG-1240B, 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-5002A, FG-5002FB2, FG-5005FA2 FortiGate DC FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-620B-DC, FG-621B-DC, FG-1240B-DC, FG-3040B-DC, FG-3140B-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC FortiGate Low Encryption FG-50B-LENC, FG-51B-LENC, FG-80C-LENC, FG-300C-LENC, FG-310B-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC, FG-5001FA2-LENC, FG-5002A-LENC FortiWiFi FWF-30B, FWF-50B, FWF-60B, FWF-60CX-ADSL-A, FWF-60CM, FWF-80CM, FWF-81CM, FWF-80CM, FWF-81CM FortiGate One FG-ONE FortiGate VM FG-VM	v4.2

Table 6: Supported FortiCarrier models

Model	Firmware Version
FortiCarrier FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5101C FortiCarrier DC FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3910B-DC, FCR-3950B-DC FortiCarrier Low Encryption FCR-5001A-DW-LENC	v5.2
FortiCarrier FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5101C FortiCarrier DC FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3950B-DC, FCR-3910B-DC FortiCarrier Low Encryption FCR-5001A-DW-LENC	v5.0

Table 6: Supported FortiCarrier models (continued)

Model	Firmware Version
FortiCarrier FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2 FortiCarrier DC FCR-3810A-DC, FCR-3950B-DC, FCR-3910B-DC FortiCarrier Low Encryption FCR-5001A-DW-LENC	v4.3
FortiCarrier FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2 FortiCarrier DC FCR-3810A-DC, FCR-3950B-DC, FCR-3910B-DC FortiCarrier Low Encryption FCR-5001A-DW-LENC	v4.2

Table 7: Supported FortiMail models

Model	Firmware Version
FortiMail FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B FortiMail VM FE-VM64	v5.1.3
FortiMail FE-100C, FE-200D, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B FortiMail VM FE-VM64	v5.0.6

Table 8: Supported FortiWeb models

Model	Firmware Version
FortiWeb FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-4000C, FWB-4000D FortiWeb VM FWB-VM64	v5.3.0 v5.2.3 v5.1.4 v5.0.6

Table 9: Supported FortiCache models

Model	Firmware Version

FortiCache
 	
    FCH-400C, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D
 	
FortiCache VM
 	
    FCH-VM64
	v3.0.0, v3.0.1

Table 10: Supported FortiSandbox models

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

Resolved Issues

The following issues have been fixed in FortiAnalyzer v5.0.9. For inquires about a particular bug, please contact Customer Service & Support.

Table 11: Resolved issues

Bug ID	Description
0257360	CVE-2014-3566 SSLv3 POODLE vulnerability. A CLI command to control the SSL protocol has been added: ```config sys global\n set ssl-protocol {tlsv1	sslv3}```
0257778	Upgraded OpenSSL for the following vulnerabilities: • CVE-2014-3513: DTLS SRTP memory leak • CVE-2014-3567: Session ticket memory leak • CVE-2014-3568: Build option no-ssl3 is incomplete • SSL 3.0 Fallback protection

Known Issues

There are no known issues in FortiAnalyzer v5.0.9. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.