



FortiAnalyzer - Release Notes

VERSION 5.2.7

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



February 2, 2017

FortiAnalyzer 5.2.7 Release Notes

05-527-369315-20160201

TABLE OF CONTENTS

Change Log	5
Introduction	6
Supported models	6
What's new in FortiAnalyzer version 5.2.7	6
Special Notices	7
Forward Compatibility with FortiOS 5.2.8 and Later	7
Manually Starting LVM Service	7
Hyper-V FortiManager-VM running on an AMD CPU	7
SSLv3 on FortiAnalyzer-VM64-AWS	7
Limited support for remote SQL database	7
SQL database rebuild	8
Device log settings	8
Log Array relocation	8
Log Arrays, devices, and VDOMs	8
Report grouping	8
Generate reports during the database rebuild	9
Special characters in report name	9
Required changes to dataset	9
FortiAnalyzer VM	10
Pre-processing logic of ebtime	10
FortiAnalyzer VM license check	10
Extended UTM log for Application Control	10
ConnectWise Management Services Platform (MSP) support	10
Distributed upgrades	11
Upgrade Information	12
Upgrading to FortiAnalyzer 5.2.7	12
Downgrading to previous versions	12
Firmware image checksums	12
FortiAnalyzer VM firmware	12
SNMP MIB files	13
Product Integration and Support	14
FortiAnalyzer version 5.2.7 support	14
Feature support	15
Language support	15

Supported models.....	16
Resolved Issues.....	23
Device Manager.....	23
Event Management.....	23
Logging.....	23
Reporting.....	23
Known Issues.....	24
Device Manager.....	24
FortiView.....	24

Change Log

Date	Change Description
2016-04-22	Initial Release.
2017-01-02	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 version 5.2.7 build 0760:

- [Supported models](#)
- [What's new in FortiAnalyzer version 5.2.7](#)
- [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 version 5.2.7 supports the following models:

FortiAnalyzer	FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B.
FortiAnalyzer VM	FAZ-VM64, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.

What's new in FortiAnalyzer version 5.2.7

The following is a list of new features and enhancements in FortiAnalyzer version 5.2.7.

- Added Report Grouping feature
- Added five new default reports to FortiCache
- Improved database rebuilding visibility
- Added *Log Insert Lag Time* and *Insert Rate vs Receive Rate* widgets
- Added Top 30 Policies by Bandwidth and Count chart for the Bandwidth and Applications Report
- FortiView menu reorganized by group
- Added Disk Usage Monitor to Resource Usage View
- Landscape view for PDF Report support

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer version 5.2.7.

Forward Compatibility with FortiOS 5.2.8 and Later

Due to log field changes, FortiAnalyzer 5.2.7 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.

Manually Starting LVM Service

If FortiAnalyzer does not have a valid Logical Volume Management (LVM) configuration, LVM service will not start on boot-up when the disk already contains data. Users will need to run `execute lvm start` to enable the service.

Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel based PC.

SSLv3 on FortiAnalyzer-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiAnalyzer-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
    set ssl-protocol tlsv1
end
```

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.

SQL database rebuild

FortiAnalyzer 5.2.2 can receive new logs during SQL database rebuild.

FortiView, Log View, Event Management, and Reports are also available. However, all scheduled reports are skipped. It is recommended to generate reports only after finishing the database rebuilding process.

Device log settings

In version 5.2.1 and later you can configure local device logging in the GUI.

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 version 5.0.6 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 version 5.2.0 or later, when selecting to add a device with VDOMs, all VDOMs are automatically added to the Log Array.

Report grouping

If you are running a large number of reports which are very similar, you can significantly improve report generation time by grouping the reports. Report grouping can reduce the number of hcache tables and improve auto-hcache completion time and report completion time.

Step 1: Configure report grouping

To group reports whose titles contain the string `Security_Report` and are grouped by device ID and VDOM, enter the following CLI commands:

```
config system report group
  edit 0
    set adom root
    config group-by
      edit devid
      next
      edit vd
      next
    end
    set report-like Security_Report
  next
end
```

Notes:

1. The `report-like` field is the name pattern of the report that will utilize the `report-group` feature. This string is case-sensitive.
2. The `group-by` value controls how cache tables are grouped.
3. To see a listing of reports and which ones have been included in the grouping, enter the following CLI command:

```
execute sql-report list-schedule <ADOM>
```

Step 2: Initiate a rebuild of hcache tables

To initiate a rebuild of hcache tables, enter the following CLI command:

```
diagnose sql rebuild-report-hcache <start-time> <end-time>
```

Where `<start-time>` and `<end-time>` are in the format: `<yyyy-mm-dd hh:mm:ss>`.

Step 3: Perform an hcache-check for a given report

Perform an hcache-check for a given report to ensure that the hcache tables exactly match the start and end time frame for the report time period. Enter the following CLI command:

```
execute sql-report hcache-check <adom> <report_id> <start-time> <end-time>
```

If you do not run this command, the first report in the report group will take a little longer to run. All subsequent reports in that group will run optimally.

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 version 5.2 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 version 5.2, 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 evertime

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 `evertime` of the current log.

In version 5.0.5 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 version 5.2.7, 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 version 5.2.

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 to FortiAnalyzer 5.2.7

You can upgrade FortiAnalyzer 5.0.6 or later directly to 5.2.7. If you are upgrading from 5.0.5 or earlier, you will need to upgrade to FortiAnalyzer 5.0.6 first.



For details about upgrading your FortiAnalyzer, see the *FortiAnalyzer Upgrade Guide*.

Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI 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 Amazon AWS, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on 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 the Open Source Xen Server.

- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the Citrix XenServer 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 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new 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 FortiManager product data sheet available on the Fortinet web site, <http://www.fortinet.com/products/fortimanager/virtual-security-management.html>. VM installation guides are available in the [Fortinet Document Library](#).

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 version 5.2.7 support

The following table lists FortiAnalyzer version 5.2.7 product integration and support information:

Web browsers	<ul style="list-style-type: none">• Microsoft Internet Explorer version 11• Mozilla Firefox version 45• Google Chrome version 49 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS/FortiOS Carrier	FortiAnalyzer 5.2.7 expects to support the following versions: <ul style="list-style-type: none">• 5.2.0 – 5.2.7 See Forward Compatibility with FortiOS 5.2.8 and Later on page 7.• 5.0.0 and later• 4.3.2 and later For the latest information, see FortiOS and FortiAnalyzer Compatibility at http://docs.fortinet.com/d/fortianalyzer-compatibility
FortiAnalyzer	<ul style="list-style-type: none">• 5.2.0 and later• 5.0.0 and later
FortiCache	<ul style="list-style-type: none">• 3.0.0 and later
FortiClient	<ul style="list-style-type: none">• 5.2.0 and later• 5.0.4 and later
FortiMail	<ul style="list-style-type: none">• 5.2.4 – 5.2.7• 5.1.6• 5.0.9
FortiManager	<ul style="list-style-type: none">• 5.2.0 and later• 5.0.0 and later
FortiSandbox	<ul style="list-style-type: none">• 1.4.0 and later
FortiWeb	<ul style="list-style-type: none">• 5.3.8• 5.2.4• 5.1.4• 5.0.6

Syslog	<ul style="list-style-type: none"> • Standard syslog
Virtualization	<ul style="list-style-type: none"> • Amazon Web Service AMI, Amazon EC2, Amazon EBS • Citrix XenServer 6.2 • Linux KVM Redhat 6.5 • Microsoft Hyper-V Server 2008 R2, 2012, and 2012 R2 • OpenSource XenServer 4.2.5 • VMware <ul style="list-style-type: none"> • ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, and 6.0



Always review the Release Notes of the supported platform firmware version before upgrading your Fortinet device.

Feature support

The following table lists FortiAnalyzer feature support for log devices.

Platform	Log View	FortiView	Event Management	Reports
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiAnalyzer	✓		✓	
FortiCache	✓		✓	✓
FortiClient	✓			
FortiMail	✓		✓	✓
FortiManager	✓		✓	
FortiSandbox	✓		✓	
FortiWeb	✓		✓	✓
Syslog	✓		✓	

Language support

The following table lists FortiAnalyzer language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
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, FortiAnalyzer, FortiMail, FortiManager, FortiWeb, FortiCache, and FortiSandbox models and firmware versions can log to a FortiAnalyzer appliance running version 5.2.7. Please ensure that the log devices are supported before completing the upgrade.

FortiGate models

Model	Firmware Version
<p>FortiGate: 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-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-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-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600C, FG-600D, FG-620B, FG-621B, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3815D, FG-3950B, FG-3951B</p> <p>FortiGate 5000 Series: FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C</p> <p>FortiGate DC: FG-80C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3950B-DC, FG-3951B-DC</p> <p>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-620B-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</p> <p>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-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D</p> <p>FortiGate Rugged: FGR-60D, FGR-100C</p> <p>FortiGate VM: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN</p> <p>FortiSwitch: FCT-5902D, FS-5203B</p>	5.2

Model	Firmware Version
<p>FortiGate: 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-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-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-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B, FGT-3000D</p> <p>FortiGate 5000 Series: FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C</p> <p>FortiGate DC: FG-80C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-1000C-DC, FG-1240B-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3950B-DC, FG-3951B-DC</p> <p>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-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC</p> <p>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-60D-3G4G-VZW, FG-70D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D</p> <p>FortiGate Rugged: FGR-60D, FGR-90D, FGR-100C</p> <p>FortiGateVoice: FGV-40D2, FGV-70D4</p> <p>FortiGate VM: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN</p> <p>FortiSwitch: FS-5203B, FCT-5903C, FCT-5913</p>	5.0

Model	Firmware Version
<p>FortiGate: 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-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</p> <p>FortiGate 5000 Series: FG-5001, FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001FA2, FG-5001FA2-LENC, FG-5002A, FG-5002A-LENC, FG-5002FB2, FG-5005FA2, FG-5005FA2-2G, FG-5005FA2-4G, FG-5101C</p> <p>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</p> <p>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-620B-LENC, FG-1000A-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</p> <p>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</p> <p>FortiGate Rugged: FGR-100C</p> <p>FortiGate One: FG-ONE</p> <p>FortiGate VM: FG-VM, FG-VM64, FG-VM64-XEN, FG-VMX</p> <p>FortiSwitch: FS-5203B</p>	4.3

FortiCarrier models

Model	Firmware Version
<p>FortiCarrier: FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5001D, FCR-5101C</p> <p>FortiCarrier DC: FCR-3240C-DC, FCR-3600C-DC, FCR-3810A-DC, FCR-3950B-DC, FCR-3951B-DC</p> <p>FortiCarrier Low Encryption: FCR-5001A-DW-LENC</p> <p>FortiCarrier VM: FCR-VM, FCR-VM64</p>	5.2

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-3950B-DC, FCR-3951B-DC FortiCarrier Low Encryption: FCR-5001A-DW-LENC FortiCarrier VM: FCR-VM, FCR-VM64	5.0
FortiCarrier: FCR-60B, FCR-60C, 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-3951B-DC FortiCarrier Low Encryption: FCR-5001A-DW-LENC	4.3

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B FortiAnalyzer VM: FAZ-VM32, FAZ-VM64, FAZ-VM64-HV	5.2
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-4000A, FAZ-4000B FortiAnalyzer VM: FAZ-VM32, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-HV	5.0

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D FortiCache VM: FCH-VM64	3.0

FortiMail models

Model	Firmware Version
FortiMail: FE-200D, FE-400C, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B FortiMail VM: FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2
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	5.1
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	5.0

FortiManager models

Model	Firmware Version
FortiManager: FMG-100C, FMG-200D, FMG-300D, FMG-300E, FMG-400C, FMG-400E, FMG-1000C, FMG-1000D, FMG-3000C, FMG-3900E, FMG-4000D, FMG-4000E FortiManager VM: FMG-VM32, FMG-VM64, FMG-VM64-AWS, FMG-VM64-HV, FMG-VM64-KVM, FMG-VM64-XEN	5.2
FortiManager: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-4000E, and FMG-5001A. FortiManager VM: FMG-VM32, FMG-VM64, FMG-VM64-HV	5.0

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-1000D, FSA-3000D FortiSandbox VM: FSA-VM	2.0 1.4

FortiWeb models

Model	Firmware Version
FortiWeb: FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000E, FWB-3000DFSX, FWB-4000C, FWB-4000D FortiWeb VM: FWB-VM64	5.3
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	5.2 5.1 5.0

Resolved Issues

The following issues have been fixed in FortiAnalyzer version 5.2.7. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Device Manager

Bug ID	Description
282491	User may not be able to delete a VDOM from Device Manager.
367006	FortiAnalyzer should not reject logs from a registered HA cluster when the slave member is removed.

Event Management

Bug ID	Description
366158	Some Email clients fail to receive Email notification from FortiAnalyzer as the MIME-Version: 1.0 header is missing.

Logging

Bug ID	Description
366011	Syslogs forwarded by FortiAnalyzer do not contain the proper FortiGate's serial number.

Reporting

Bug ID	Description
366005	When editing the Top 30 application chart, it does not show the Data Bindings section.
367016	FortiAnalyzer cannot generate report based on Top 5 user per bandwidth.

Known Issues

The following issues have been identified in FortiAnalyzer version 5.2.7. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Device Manager

Bug ID	Description
279319	Device Manager may display non-existing VDOMs with strange characters.

FortiView

Bug ID	Description
356073	FortiView has a discrepancy between FortiGate and FortiAnalyzer regarding the sent/received bytes value.



Copyright© 2016 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.