



FortiAnalyzer Release Notes

VERSION 5.2.3

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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 5.2.3 Release Notes

05-523-285708-20170201

TABLE OF CONTENTS

Change Log	5
Introduction	6
Supported models	6
Special Notices	7
Forward Compatibility with FortiOS 5.2.8 and Later	7
SSLv3 on FortiAnalyzer-VM64-AWS	7
Limited support for remote SQL database	7
SQL database rebuild	7
Device log settings	7
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	9
Pre-processing logic of eptime	9
FortiAnalyzer VM license check	10
Extended UTM log for Application Control	10
ConnectWise Management Services Platform (MSP) support	10
Distributed upgrades	10
Upgrade Information	11
Upgrading from FortiAnalyzer version 5.2.0, 5.2.1, & 5.2.2	11
Upgrading from FortiAnalyzer version 5.0.6 or later	11
Downgrading to previous versions	11
Firmware image checksums	11
FortiAnalyzer VM firmware	11
SNMP MIB files	12
Product Integration and Support	13
FortiAnalyzer version 5.2.3 support	13
Feature support	14
Language support	15
Supported models	16

Resolved Issues	22
Known Issues	25

Change Log

Date	Change Description
2015-07-30	Initial Release.
2015-08-10	Added Microsoft Hyper-V Server 2012 R2 to Product Integration and Support.
2015-11-19	Added 274240 to Resolved Issues.
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 version 5.2.3 build 724:

- [Supported models](#)
- [Introduction](#)
- [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 5.2.3 supports the following models:

FortiAnalyzer	FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-1000C, FAZ-1000D, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-3900E, and FAZ-4000B.
FortiAnalyzer VM	FAZ-VM32, FAZ-VM64, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer version 5.2.3.

Forward Compatibility with FortiOS 5.2.8 and Later

Due to log field changes, FortiAnalyzer 5.2.3 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.

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 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 `devvid`, `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 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 5.2.3, 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 from FortiAnalyzer version 5.2.0, 5.2.1, & 5.2.2

FortiAnalyzer version 5.2.3 supports upgrade from version 5.2.0, 5.2.1 & 5.2.2.

Upgrading from FortiAnalyzer version 5.0.6 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.



For information on 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-bits Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bits firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.OpenXen.zip`: Download the 64-bits 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-bits package for a new FortiAnalyzer VM installation. This package contains the Citrix XenServer Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bits firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.kvm.zip`: Download the 64-bits 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 VM installation.
- `.ovf.zip`: Download either the 32-bit or 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/virtualappliances.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 5.2.3 support

The following table lists FortiAnalyzer version 5.2.3 product integration and support information:

Web browsers	<ul style="list-style-type: none">• Microsoft Internet Explorer version 11• Mozilla Firefox version 39• Google Chrome version 43 <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
FortiOS/FortiOS Carrier	<ul style="list-style-type: none">• 5.2.0–5.2.7 <p>See Forward Compatibility with FortiOS 5.2.8 and Later on page 7.</p> <ul style="list-style-type: none">• 5.0.0 and later• 4.3.2 and later
FortiAnalyzer	<ul style="list-style-type: none">• 5.2.3• 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• 5.1.5• 5.0.8
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">• 5.3.7• 5.2.4• 5.1.4• 5.0.6
Syslog	<ul style="list-style-type: none">• Standard syslog

Virtualization

- 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

- 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.

Feature support per platform

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 support

Language	GUI	Reports	Documentation
English	✓	✓	✓
Chinese (Simplified)	✓	✓	
Chinese (Traditional)	✓	✓	
French		✓	
Hebrew		✓	
Hungarian		✓	
Japanese	✓	✓	
Korean	✓	✓	
Portuguese		✓	
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, FortiAnalyzer, FortiMail, FortiManager, FortiWeb, FortiCache, and FortiSandbox models and firmware versions can log to a FortiAnalyzer appliance running version 5.2.3. Please ensure that the log devices are supported before completing the upgrade.

Supported FortiGate models

Model	Firmware Version
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-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-620B, FG-621B, FG-800C, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3950B, FG-3951B	5.2
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	
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-3700D-DC, FG-3810A-DC, FG-3810D-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-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D	
FortiGate Rugged: FGR-60D, FGR-100C	
FortiGate VM: FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN	
FortiSwitch: FS-5203B	

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-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3016B, FG-3040B, 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-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-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-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC</p>	5.0
<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-HV, FG-VM64-KVM, FG-VM64-XEN</p>	
<p>FortiSwitch: FS-5203B, FCT-5903C, FCT-5913</p>	

Model	Firmware Version
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 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 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	4.3

Supported FortiCarrier models

Model	Firmware Version
FortiCarrier: FCR-3240C, FCR-3600C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5001D, 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	5.2

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	5.0
FortiCarrier Low Encryption: FCR-5001A-DW-LENC	
FortiCarrier VM: FCR-VM, FCR-VM64	
FortiCarrier: FCR-60B, FCR-60C, FCR-3810A, FCR-3950B, FCR-3951B, FCR-5001, FCR-5001A, FCR-5001B, FCR-5001FA2, FCR-5005FA2	4.3
FortiCarrier DC: FCR-3810A-DC, FCR-3950B-DC, FCR-3951B-DC	
FortiCarrier Low Encryption: FCR-5001A-DW-LENC	

Supported FortiAnalyzer models

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

Supported FortiCache models

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

Supported 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

Supported FortiManager models

Model	Firmware Version
FortiManager: FMG-100C, FMG-200D, FMG-300D, FMG-400C, 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

Supported FortiSandbox models

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

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

Resolved Issues

The following issues have been fixed in FortiAnalyzer version 5.2.3. For inquiries about a particular bug, please contact [Customer Service & Support](#).

GUI

Bug ID	Description
266262	FortiAnalyzer does not flush duplicated queries from the FortiGate.
270656	FortiAnalyzer displays incorrect FortiOS firmware version after upgrading the FortiGate's firmware.
283832	FortiAnalyzer keeps updating addresses from multiple VDOMs when the FortiAnalyzer override option is enabled on FortiGate.
279319	FortiAnalyzer displays non-existing VDOMs with strange characters.

Event Management

Bug ID	Description
229083	Devices in Event Handlers are not updated when the device is modified.
265993	SNMPv3 profile is not supported in Event Management.
270264	Change the Device ID to Device Name in the Email subject line.

FortiView

Bug ID	Description
280181	FortiAnalyzer does not display IP/MAC information in the DHCP logs.

Logging

Bug ID	Description
264233	When logging a generic syslog device to the FortiAnalyzer, and then try to display logs, the message field has a fixed size and cannot adapt to the column size.
276491	After upgrading, the FortiAnalyzer is missing GTP specific fields in the event log viewer.
278077	Traffic log table still displays the Date/Time column even though it has been disabled via <i>Column Settings</i> .

Bug ID	Description
278804	FortiAnalyzer does not restrict the number for Last N days in <i>Log View</i> .
280053	<i>Attack Context ID for Intrusion Prevention</i> logs are not parsed properly.
280192	Base64 encoded <code>log-attack-context</code> events are not readable.
280891	When viewing FortiSandbox logs, several fields are missing.
281953	Advanced ADOM mixes up logs from different VDOMs.
284658	The <i>GO</i> button does not refresh logs on the Log View summary page.
280873	String value in the extension field formatted using CEF is surrounded by quotes.
274240	Improve log aggregation speed.

Other

Bug ID	Description
273477	FortiAnalyzer is unable to extend the device quota via CLI.
273533	FortiAnalyzer should assign <code>sqllogd</code> more efficiently when there are not many devices.
274233	FortiAnalyzer cannot backup logs to a Linux server.
276904	Status is not correct when rebuilding the database.
279760	FortiAnalyzer returns an error when running <code>searchFazLog</code> using <i>duration</i> or <i>sentbyte</i> as the <code>searchCriteria</code> with XML API.
277478	The <code>pgsvr.log</code> shows many: <i>ERROR: extra data after last expected column</i> messages.

Reporting

Bug ID	Description
205028	Historical Report list cannot be retrieved after changing the ADOM name.
262593	Japanese characters in a PDF formatted report are displayed in an unexpected font style.
275394	When the dataset is changed, the FortiAnalyzer loses the auto column update in the chart.
276050	Report for FortiMail displays <i>Unknown</i> or missing outputs.

Bug ID	Description
276715	Improve the speed when loading report lists from the main menu.
276722	Improve the speed when loading the Calendar.
279681	Users cannot filter category for predefined reports with the <i>Chart Filter</i> .
284133	Start time and End time are not correct in SQL when <code>\$flex_timescale</code> is used.
257691	Report line chart limits number of items depending on the period of the report.

System Settings

Bug ID	Description
278334	FortiAnalyzer displays inconsistent behavior for read-only admin profiles.

Known Issues

The following issues have been identified in FortiAnalyzer version 5.2.3. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

GUI

Bug ID	Description
283818	When editing a device to enable the HA and add a slave to the cluster, the new HA members may not be correctly added.

Logging

Bug ID	Description
286804	Log search may be slower than expected and may return unexpected results.

Others

Bug ID	Description
284909	The <code>xml.wsdl</code> file may not be parsed by external libraries correctly.
286498	FortiAnalyzer may be unable to backup log to the FTP when the <code>log-file-archive-name</code> is set to <i>extended</i> .

