FortiAnalyzer Release Notes

VERSION 5.2.1

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 01, 2017

FortiAnalyzer 5.2.1 Release Notes

05-521-261302-20170201

TABLE OF CONTENTS

Change Log

Date	Change Description
2014-12-12	Initial release.
2014-12-15	Minor document updates.
2014-12-19	Added 0252654 and 0252059 to the Resolved Issues chapter. Other minor document updates.
2015-01-09	Minor document updates.
2015-02-04	Added a remote SQL database special notice.
2015-04-13	Change to Upgrade Information chapter.
2015-04-30	Added VM Partition and Firmware Information to the Upgrade Information chapter.
2015-06-02	Updated Upgrade Information Chapter.
2017-02-01	Added *Special Notices > Forward Compatibility with FortiOS 5.2.8 and Later*. Updated *Product Integration and Support > FortiOS/FortiOS Carrier*.

Introduction

This document provides the following information for FortiAnalyzer version 5.2.1 build 0662:

For more information on upgrading your FortiAnalyzer device, see the *FortiAnalyzer Upgrade Guide*.

Supported models

FortiAnalyzer version 5.2.1 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, FAD-VM64, and FAZ-VM64-HV.

What's new in FortiAnalyzer version 5.2.1

The following is a list of new features and enhancements in FortiAnalyzer version 5.2.1.

FortiView

- View for SSL & Dialup IPSec Events
- View for System & Admin Login Events
- View for Rogue APs
- View for Site-to-Site IPsec VPN
- View for Firewall Resource Usage

Log View

- FortiAnalyzer, FortiCache, FortiManager, FortiSandbox, FortiWeb, and syslog log forwarding support
- Support reverse order in log viewer
- FortiClient log support
- Stacked bar for Threat View

Event Management

- FortiAnalyzer, FortiCache, FortiManager, FortiSandbox, FortiWeb, and syslog support
- New default event handlers

Reports

- New WYSIWYG report editor
- Tool for validating custom datasets
- New Application Risk and Control report

Other

- Added a CLI command to erase data on disk
- Added support for device registration for FortiManager and FortiAnalyzer in DVM table
- Log file range has been changed to 10-500MB. The default value is 100MB.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer version 5.2.1.

Forward Compatibility with FortiOS 5.2.8 and Later

Due to log field changes, FortiAnalyzer 5.2.2 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.

SQL database rebuild

Upgrading the device firmware can trigger an SQL database rebuild. During this time, new logs will not be available until the rebuild is complete. The time required to rebuild the database is dependent on the size of the database. You can use the `diagnose sql status rebuild-db` command to display the SQL log database rebuild status.

The following features will not be available until after the SQL database rebuild has completed: FortiView, Log View, Event Management, and Reports.

Device log settings

In version 5.2.1 and later you can configure local device logging in the Web-based Manager.

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.

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 `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 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 5.2.1, 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

FortiAnalyzer version 5.2.1 supports upgrade from version 5.2.0.

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 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 Microsoft Hyper-V Server and VMWare ESX/ESXi 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 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 5.2.1 support

The following table lists FortiAnalyzer version 5.2.1 product integration and support information:

Web browsers	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 35 • Google Chrome version 40 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 5.2.0-5.2.7 See Forward Compatibility with FortiOS 5.2.8 and Later on page 8 • 5.0.0 and later • 4.3.2 and later
FortiAnalyzer	• 5.2.0 and later • 5.0.0 and later
FortiCache	• 3.0.0 and later
FortiClient	• 5.2.0 and later • 5.0.4 and later
FortiMail	• 5.2.2 • 5.1.4 • 5.0.7
FortiManager	• 5.2.0 and later • 5.0.0 and later
FortiSandbox	• 1.4.0 and later
FortiWeb	• 5.3.3 • 5.2.4 • 5.1.4 • 5.0.6
Syslog	• Standard Syslog

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

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	Web-based Manager	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 5.2.1. 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-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-3700DX, FG-3810A, FG-3950B, FG-3951B **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-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 **FortiGate Rugged:** FGR-60D, FGR-100C **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B	5.2

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-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 **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-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, FWF-60D-POE, FWF-60D-3G4G-VZW, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate Rugged:** FGR-60D, FGR-90D, FGR-100C **FortiGateVoice:** FGV-40D2, FGV-70D4 **FortiGate VM**: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B	5.0

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

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 **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-HV	5.0

Supported FortiCache models

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

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-HV	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 **FortiSandbox VM:** FSA-VM	2.0 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 **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 5.2.1. For inquires about a particular bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
0217410	FortiAnalyzer does not support logs sent by FortiManager.
0229751	Syslog Forwarding causes the device ID to change after upgrading FortiAnalyzer.
0251909	FortiCarrier VDOMs are not displayed in the Device Manager.
0255192	FortiGate device is not shown under Device Manager when FortiGate is in demo mode.

Event Management

Bug ID	Description
0218025	Additional information field does not show relevant data for web filter and application control.
0246951	FortiAnalyzer may send an alert notification email with null body.
0252342	Event Management's IPS handlers put the handler name under the Event Name column.
0254298	When a SQL database is rebuilt, all past events under Events Management are re-sent.

Logging

Bug ID	Description
0222312	FortiAnalyzer cannot archive files from HTTPS sessions.
0228960	FortiAnalyzer cannot generate a report with more than 1500 rows.
0242781	Email archive has been marked even though an email has no attachment.
0250095	After upgrading FortiAnalyzer, it takes longer to generate a report even though `auto-hcache` is enabled.
0251828	The `unauthuser` field information from FortiClient is not populated on FortiView's source column.

Bug ID	Description
0252059	Log forwarding currently only supports FortiGate, FortiMail, and FortiWeb. The Web-based Manager and CLI options do not match.
0252844	Policy ID is not displayed for security logs.
0252911	Custom View of syslog log records does not return any data.

Other

Bug ID	Description
0239052	The `execute log device disk_quota` CLI command does not display all devices.
0243858	The OFTP daemon may frequently crash.
0248969	FortiGate receives incorrect disk space information when testing FortiAnalyzer's connectivity.
0250849	Added a CLI option to disable TCP port 541.
0252654	FortiAnalyzer does not send logs to CEF server.
0252883	FortiAnalyzer is not able to input the `AND` condition with both source and destination interfaces with VLAN filter from the `runFazReport` request.
0253087	The `lvr_debug.txt` file consumes too much disk space.
0255993	Many empty cloned child tables are inserted into database.
0257160	The `sqlreportd` daemon reports a `Failed to connect to path /tmp/sql_plugin` error after upgrade, and detects an invalid SQL error during SQL database upgrade.
0259522	Reports or output profiles are lost after upgrade.

Reporting

Bug ID	Description
0216903	FortiClient log report and view should be supported.
0226027	User should be able to add multiple filters with the same field name with different value.
0236964	FortiAnalyzer cannot create a report with a carrier end point value filter applied.
0252921	FortiAnalyzer does not send out report via email.
0253687	Y-Axis scale is overlapped when hostname is too long.

Bug ID	Description
0253837	When multiple headings of the same type exist, the second one is always indented.
0254142	FortiAnalyzer queries incorrect results when LDAP group filter is used.
0254418	Wildcard does not work on `srcip` filter.
0254690	When trying to backup generated reports, FortiAnalyzer only pushes a 45byte file to the remote server.
0255543	FortiAnalyzer should not show logs that are sent by `invalid device`.
0257385	FortiAnalyzer is unable to remove Appendix A from report when filters are used.

Known Issues

The following issues have been identified in FortiAnalyzer version 5.2.1. For inquires about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Event Management

Bug ID	Description
0258225	Event Management mail fails when remote Novell MTA is configured.

Logging

Bug ID	Description
0260639	All log entries are downloaded if *Now* is selected as the *End Time* on custom time period.
0261532	FortiClient logs are not forwarded to the remote aggregation
0263885	After upgrade, old FortiClient log files are not available in the new FortiClient log view.