FortiAnalyzer - Release Notes

Version 5.6.3

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

June 28, 2018
FortiAnalyzer 5.6.3 Release Notes
05-563-477274-20180628

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-03-15	Initial release of 5.6.3.
2018-03-23	Added special notice about Mixed HA groups.
2018-06-28	Added support for FortiOS 5.6.5

Introduction

This document provides the following information for FortiAnalyzer version 5.6.3 build 1662:

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

Supported models

FortiAnalyzer version 5.6.3 supports the following models:

FortiAnalyzer	FAZ-200D, FAZ-200F, FAZ-300D, FAZ-300F, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F and FAZ-3900E.
FortiAnalyzer VM	FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).

Minimum screen resolution

The recommended minimum screen resolution is 1280 x 800. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer version 5.6.3.

Mixed HA groups

FortiAnalyzer uses the High Availability (HA) group name to create and register FortiGate devices in Device Manager. When multiple FortiGate clusters use the same group name, they appear as one, mixed cluster in the *Device Manager* pane in FortiAnalyzer GUI. The solution is to disable automatic grouping of HA members in FortiAnalyzer and clean up the mixed cluster.

Automatic grouping of HA members is enabled by default in FortiAnalyzer.

The following example describes how to clean up a mixed cluster in FortiAnalyzer that contains two FortiGate clusters.

To disable automatic grouping of HA members:

1. Log on to FortiAnalyzer and run the following command:
```
conf sys global
set ha-member-auto-grouping disable
end
```

To clean up the mixed cluster:

1. From FortiOS GUI, identify the High Availability (HA) primary and secondary members for the two clusters, according to the FortiGate HA infrastructure.
2. In FortiAnalyzer GUI, clean up the mixed HA cluster by deleting the HA members for the second HA cluster.
   a. Go to *Device Manager*.
   b. Right-click the HA cluster and select *Edit*.
   c. Click the *Delete* icon to delete the members that do not belong to this cluster.

   The result is one HA cluster with the required devices. The deleted devices for the second cluster are displayed in the *Unregistered device* list.
3. From FortiAnalyzer CLI, delete all the VDOM names from the mixed HA cluster by using the `exe log device vdom delete <Device Name> <VDOM>` command.
4. From FortiAnalyzer GUI, verify and promote unregistered devices to the second cluster.
   a. Go to *Device Manager*, and verify that the deleted devices for the second HA cluster are displayed in the *Unregistered device* list as separate HA devices.
   b. Promote the unregistered HA devices as HA devices.
5. In *Device Manager*, clean up the second cluster.
   a. Right-click the secondary device in the second cluster, and select *Edit*.
   b. Clear the *HA Cluster* check box to convert the secondary device to a standalone device.

c. Right-click the primary device in the second cluster, and select *Edit*.
d. Add the secondary device back to the cluster.

6. In FortiAnalyzer, verify that there is a proper VDOM on the second cluster. If not, follow step 3 to delete the mixed VDOM by using the CLI.
7. From FortiAnalyzer GUI, go to *Device Manager*, and press F5 to load all the VDOMs into the GUI.

Hyper-V FortiAnalyzer-VM running on an AMD CPU

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

IPsec connection to FortiOS for logging

FortiAnalyzer 5.4.2 and later does not support an IPsec connection with FortiOS 5.0/5.2. However UDP or TCP + reliable are supported.

Instead of IPsec, you can use the FortiOS reliable logging feature to encrypt logs and send them to FortiAnalyzer. You can enable the reliable logging feature on FortiOS by using the `configure log fortianalyzer setting` command. You can also control the encryption method on FortiOS by using the `set enc-algorithm default/high/low/disable` command.

Datasets Related to Browse Time

If upgrading from an image prior to FAZ 5.4.2, cloned datasets that query for browse time may not be able to return any results after upgrade.

FortiAnalyzer 5.4.2 contains enhancements to calculating the estimated browse time. Due to the changes, cloned datasets that query for browse time may not be able to return any results after upgrade.

System Configuration or VM License is Lost after Upgrade

When upgrading FortiAnalyzer from 5.4.0 or 5.4.1 to 5.4.x or 5.6.0, it is imperative to reboot the unit before installing the 5.4.x or 5.6.0 firmware image. Please see the *FortiAnalyzer Upgrade Guide* for details about upgrading. Otherwise, FortiAnalyzer may lose system configuration or VM license after upgrade. There are two options to recover the FortiAnalyzer unit:

1. Reconfigure the system configuration or add VM license via CLI with `execute add-vm-license <vm license>`.
2. Restore the 5.4.0 backup and upgrade to 5.4.2.

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 t1sv1
end
```

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.

Port 8443 reserved

Port 8443 is reserved for `https-logging` from FortiClient EMS for Chromebooks.

Upgrade Information

Upgrading to FortiAnalyzer 5.6.3

You can upgrade FortiAnalyzer 5.4.0 or later directly to 5.6.3.

If you are upgrading from versions earlier than 5.4.0, you must upgrade to FortiAnalyzer 5.4 first. (We recommend that you upgrade to 5.4.5, the latest version of FortiAnalyzer 5.4.)

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

ESX VM network mapping after upgrade

Starting with FortiAnalyzer 5.6.0, Fortinet changed the network interface mapping as shown below. After upgrade to FortiAnalyzer 5.6.3, you must edit ESX VM network mapping in order to preserve network connectivity.

- port1 -> Network Adapter 1
- port2 -> Network Adapter 2
- port3 -> Network Adapter 3
- port4 -> Network Adapter 4

New FortiAnalyzer 5.6.0 and later VM installations use the correct mapping with ESX 5.5 and later.

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, Citrix and Open Source XenServer, Linux KVM, 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 Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FAZ_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.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 Azure.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FAZ_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.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.

Microsoft Hyper-V 2016 is supported.

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 5.6.3 support

The following table lists FortiAnalyzer version 5.6.3 product integration and support information:

Web Browsers	• Microsoft Internet Explorer version 11 or Edge 40 Due to limitation on Microsoft Internet Explorer or Edge, it may not completely render a page with a large set of policies or objects. • Mozilla Firefox version 57 • Google Chrome version 63 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS/FortiOS Carrier	• 5.6.0 to 5.6.5 • 5.4.0 to 5.4.8 • 5.2.0 to 5.2.13
FortiAnalyzer	• 5.6.0 to 5.6.3 • 5.4.0 to 5.4.3 • 5.2.0 to 5.2.9 • 5.0.0 to 5.0.13
FortiCache	• 4.2.6 • 4.1.3 • 4.0.4
FortiClient	• 5.6.0 and later • 5.4.0 and later • 5.2.0 and later • 5.0.4 and later
FortiMail	• 5.4.4 • 5.3.11 • 5.2.9 • 5.1.6 • 5.0.10
FortiManager	• 5.6.0 to 5.6.3 • 5.4.0 to 5.4.3 • 5.2.0 and later • 5.0.0 and later

FortiSandbox	• 2.5.1 • 2.5.0 • 2.4.1 • 2.4.0 • 2.3.3 • 2.3.2 • 2.2.2 • 2.1.3 • 2.0.3 • 1.4.0 and later • 1.3.0 • 1.2.0 and 1.2.3
FortiSwitch ATCA	• 5.0.0 and later • 4.3.0 and later • 4.2.0 and later
FortiWeb	• 5.8.6 • 5.8.3 • 5.8.1 • 5.8.0 • 5.7.0 • 5.6.0 • 5.5.4 • 5.4.1 • 5.3.8 • 5.2.4 • 5.1.4 • 5.0.6
FortiDDoS	• 4.5.0 • 4.4.1 • 4.2.3 • 4.1.12
FortiAuthenticator	• 5.2.1 • 5.1.0 • 5.0.0 • 4.3.0 • 4.2.0 • 4.1.0 • 4.0.0

Virtualization	• Amazon Web Service AMI, Amazon EC2, Amazon EBS
	• Citrix XenServer 6.2
	• Linux KVM Redhat 6.5
	• Microsoft Azure
	• Microsoft Hyper-V Server 2008 R2, 2012 & 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, 6.0 and 6.5

Always review the Release Notes of the supported platform firmware version before upgrading your 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 registered to FortiGate	✓	✓		✓
FortiClient registered to FortiClient EMS	✓	✓		✓
FortiDDoS	✓	✓	✓	✓
FortiMail	✓		✓	✓
FortiManager	✓		✓	
FortiSandbox	✓		✓	✓
FortiWeb	✓		✓	✓
Syslog	✓		✓	

FortiGate Management

You can enable FortiManager features on some FortiAnalyzer models. FortiAnalyzer models with FortiManager features enabled can manage a small number of FortiGate devices, and all but a few FortiManager features are enabled on FortiAnalyzer. The following table lists the supported modules for FortiAnalyzer with FortiManager Features enabled:

FortiManager Management Modules	FortiAnalyzer with FortiManager Features Enabled
Device Manager, except firmware and license management	✓
Policy & Objects	✓
AP Manager	✓
FortiClient Manager	✓
VPN Manager	✓
FortiGuard	
FortiMeter	
FGT-VM License Activation	
Chassis Management	✓

Language support

The following table lists FortiAnalyzer language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Hebrew		✓
Hungarian		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Russian		✓

Language	GUI	Reports
Spanish		✓

To change the FortiAnalyzer language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language from the drop-down list. 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, FortiDDoS, FortiAnalyzer, FortiMail, FortiManager, FortiWeb, FortiCache, and FortiSandbox models and firmware versions can log to a FortiAnalyzer appliance running version 5.6.3. Please ensure that the log devices are supported before completing the upgrade.

Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

FortiGate models

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C,FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, **FortiGate 5000 Series:** FG-5001C, FG-5001D **FortiGate DC:** FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC **FortiGate Low Encryption:** FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC **FortiWiFi:** FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate VM:** FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN, FG-VMX-Service-Manager, FOSVM64, FOSVM64-KVM **FortiGate Rugged:** FGR-30D, FGR-35D, FGR-60D, FGR-90D	5.6

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE,FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-200E, FG-201E, FGT-300D, FGT-300E, FGT-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG 3800D, FG-3810D, FG-3815D, FG-3960E, FG3980E, FG-2000E, FG-2500E **FortiGate 5000 Series:** FG-5001C, FG-5001D, FG-5001E, FG-5001E1 **FortiGate 7000 Series:** FG-7030E-Q, FG-7030E-S, FG-7040E-1, FG-7040E-2, FG-7040E-3, FG-7040E-4, FG-7040E-5, FG-7040E-6, FG-7040E-8, FG-7040E-8-DC, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6, FG-7060E-8 **FortiGate DC:** FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815DC **FortiGate Low Encryption:** FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC **FortiWiFi:** FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E-DSL, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D **FortiGate VM:** FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM **FortiGate Rugged:** FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D	5.4

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-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-3000D, 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 **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-800D-DC, FG-1000C-DC, FG-1240B-DC, FG-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, G-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3815D-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-620B-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-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-AWSONDEMAND, FG-VM-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN **FortiSwitch:** FS-5203B, FCT-5902D	5.2

FortiCarrier Models

Model	Firmware Version
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3700D, FCR-3700DX, FCR-3800D, FCR-3810D, FCR-3815D, FCR-5001C, FCR-5001D, FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C, FCR-3600C, FCR-3700D-DC, FCR-3810D-DC, FCR-5001C **FortiCarrier DC:** FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C-DC, FCR-3600C-DC, FCR-3700D-DC, FCR-3810D-DC, FCR-3815D-DC **FortiCarrier VM:** FCR-VM, FCR-VM64, FCR-VM64-AWS, FCR-VM64-AWSONDEMAND, FCR-VM64-HV, FCR-VM64-KVM	5.4

Model	Firmware Version
FortiCarrier: FCR-3000D, FCR-3100D, FCR-3200D, FCR-3240C, FCR-3600C, FCR-3700D, FCR-3700DX, FCR-3810A, FCR-3810D, FCR-3815D, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C,FCR-5001D, FCR-5101C, FCR5203B, FCR-5902D **FortiCarrier DC:** FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3700D-DC, FCR-3810D-DC **FortiCarrier Low Encryption:** FCR-5001A-DW-LENC **FortiCarrier VM:** FCR-VM, FCR-VM64, FCR-VM64-HV, FCR-VM64-KVM, FCR-Vm64-XEN, FCR-VM64-AWSONDEMAND	5.2

FortiDDoS models

Model	Firmware Version
FortiDDoS: FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B	4.2, 4.1, 4.0

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	5.6
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B. **FortiAnalyzer VM:** FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-200E, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
FortiAnalyzer: FAZ-100C, FAZ-200D, FAZ-200E, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B **FortiAnalyzer VM:** FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

FortiMail models

Model	Firmware Version
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B **FortiMail Low Encryption:** FE-3000C-LENC **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3.7
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B **FortiMail VM:** FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2.8
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.1.6
FortiMail: FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B **FortiMail VM:** FE-VM64	5.0.10

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D **FortiSandbox VM:** FSA-VM	2.4.0 2.3.2
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D **FortiSandbox VM:** FSA-VM	2.2.0 2.1.0
FortiSandbox: FSA-1000D, FSA-3000D **FortiSandbox VM:** FSA-VM	2.0.0 1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

FortiSwitch ACTA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-59	5.2.0
FortiSwitch-ATCA: FS-5003A, FS-5003B **FortiController:** FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3.0 4.2.0

FortiWeb models

Model	Firmware Version
FortiWeb: FWB-2000E	5.6.0
FortiWeb: FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.3
FortiWeb: FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, FWB-HYPERV	5.4.1
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER, and FWB-HYPERV	5.3.8
FortiWeb: FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E **FortiWeb VM:** FWB-VM64, FWB-HYPERV,FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVER	5.2.4

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E **FortiCache VM:** FCH-VM64, FCH-KVM	4.1
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E **FortiCache VM:** FCH-VM64	4.0

Resolved Issues

The following issues have been fixed in FortiAnalyzer version 5.6.3. For inquires about a particular bug, please contact Customer Service & Support.

Device Manager

Bug ID	Description
469903	FortiGate cluster devices with a same group name may be mixed up under Device Manager.
464691	When adding the serial number for FortiSandbox-VM, FortiAnalyzer reports the platform as a FortiSandbox-1000D.
469992	When there are multiple VDOMs on a FortiGate device, only one VDOM's log file is deleted when quota policy is enforced.

Event Management

Bug ID	Description
464677	The *Show Related Logs* and *Show Triggered History* menu options return web server error 500 when the event name contains a special character.
476749	FortiAnalyzer may render log details on events triggered by email filter logs.

Log View

Bug ID	Description
470516	The `oftpd` process may stop responding.
460430	FortiAnalyzer may not return any results when filtering on *Serial Number* with `device_id=FG`.

Known Issues

The following issues have been identified in FortiAnalyzer version 5.6.3. For inquires about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Device Manager

Bug ID	Description
481694	We do not have a different *Unregistered* buttons for different device types and for different ADOMs. This is because we do not identify different devices types (for example, FortiGate or FortiMail) for unregistered devices. FortiOS 5.4 has an existing issue where a non-root ADOM always shows 0 and the button is grayed out. FortiOS 5.6 has an existing issue where a non-root ADOM shows the number of unregistered devices, but clicking it does not do anything and you are not automatically redirected to the root ADOM.

Event Management

Bug ID	Description
470373	During database rebuilds, alerts that are already triggered may be replayed again.

Log View

Bug ID	Description
455739	When filtering by device, syslog ADOM may not correctly show logs that belong to the same device.
465378	*Subject Filter* in Log View may not work with 2-byte characters of FortiMail logs.

Reports

Bug ID	Description
470616	Entries may overlap in the reports generated in PDF format.

Bug ID	Description
476645	Output Profile may limit SFTP password length to 31 characters.

System settings

Bug ID	Description
474066	When an administrator profile is configured with Read-Write permission for Reports and Read-Only for System Settings, administrators associated with the profile cannot preview or save a chart using chart builder.
474935	Chromebooks stops logging to FortiAnalyzer when HTTP access is not allowed on network interface.
476701	Log forwarding sends logs with a missing double quote at the end of the `poluuid` value.