

# FortiAnalyzer - Release Notes

Version 5.6.7

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



December 6, 2018

FortiAnalyzer 5.6.7 Release Notes

05-567-526110-20181206

# TABLE OF CONTENTS

<b>Change Log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
Supported models	5
Minimum screen resolution	5
<b>Special Notices</b>	<b>6</b>
Mixed HA groups	6
Hyper-V FortiAnalyzer-VM running on an AMD CPU	7
IPsec connection to FortiOS for logging	7
Datasets Related to Browse Time	7
System Configuration or VM License is Lost after Upgrade	7
SSLv3 on FortiAnalyzer-VM64-AWS	8
Pre-processing logic of eftime	8
Port 8443 reserved	8
<b>Upgrade Information</b>	<b>9</b>
Upgrading to FortiAnalyzer 5.6.7	9
ESX VM network mapping after upgrade	9
Downgrading to previous versions	9
Firmware image checksums	9
FortiAnalyzer VM firmware	10
SNMP MIB files	11
<b>Product Integration and Support</b>	<b>12</b>
FortiAnalyzer version 5.6.7 support	12
Feature support	14
FortiGate Management	15
Language support	15
Supported models	16
<b>Resolved Issues</b>	<b>24</b>
FortiView	24
Log View	24
Reports	24
System Settings	24
Others	25
Common Vulnerabilities and Exposures	25
<b>Known Issues</b>	<b>26</b>
FortiView	26
Log View	26
Others	26

# Change Log

Date	Change Description
2018-12-06	Initial release of 5.6.7.

# Introduction

This document provides the following information for FortiAnalyzer version 5.6.7 build 1782:

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

<b>FortiAnalyzer</b>	FAZ-200D, FAZ-200F, FAZ-300D, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000D, FAZ-1000E, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F and FAZ-3900E.
<b>FortiAnalyzer VM</b>	FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, 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 5.6.7.

## 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 tlsv1
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 5.6.7

You can upgrade FortiAnalyzer 5.4.0 or later directly to 5.6.7. If you are upgrading from versions earlier than 5.4.x, you should upgrade to the latest patch version of FortiAnalyzer 5.4 first.



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 5.6.7, 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.

### Google GCP

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.gcp.zip`: Download the 64-bit package for a new FortiManager VM installation.

### 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 5.6.7 support

The following table lists FortiAnalyzer version 5.6.7 product integration and support information:

<b>Web Browsers</b>	<ul style="list-style-type: none"><li>• 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.</li><li>• Mozilla Firefox version 63</li><li>• Google Chrome version 70</li></ul> Other web browsers may function correctly, but are not supported by Fortinet.
<b>FortiOS/FortiOS Carrier</b>	<ul style="list-style-type: none"><li>• 5.6.0 to 5.6.7</li><li>• 5.4.0 to 5.4.10</li><li>• 5.2.0 to 5.2.13</li></ul>
<b>FortiAnalyzer</b>	<ul style="list-style-type: none"><li>• 5.6.0 and later</li><li>• 5.4.0 and later</li><li>• 5.2.0 and later</li><li>• 5.0.0 and later</li></ul>
<b>FortiCache</b>	<ul style="list-style-type: none"><li>• 4.2.8</li><li>• 4.1.6</li><li>• 4.0.4</li></ul>
<b>FortiClient</b>	<ul style="list-style-type: none"><li>• 5.6.0 and later</li><li>• 5.4.0 and later</li><li>• 5.2.0 and later</li><li>• 5.0.4 and later</li></ul>
<b>FortiMail</b>	<ul style="list-style-type: none"><li>• 5.4.7</li><li>• 5.3.12</li><li>• 5.2.10</li><li>• 5.1.7</li><li>• 5.0.10</li></ul>
<b>FortiManager</b>	<ul style="list-style-type: none"><li>• 5.6.0 and later</li><li>• 5.4.0 and later</li><li>• 5.2.0 and later</li><li>• 5.0.0 and later</li></ul>

- FortiSandbox**
- 2.5.2
  - 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**
- 5.2.5

- FortiWeb**
- 5.9.1
  - 5.8.6
  - 5.8.3
  - 5.8.1
  - 5.8.0
  - 5.7.2
  - 5.6.1
  - 5.5.6
  - 5.4.1
  - 5.3.9
  - 5.2.4
  - 5.1.4
  - 5.0.6

- FortiDDoS**
- 4.6.0
  - 4.5.0
  - 4.4.2
  - 4.3.2
  - 4.2.3
  - 4.1.12

- FortiAuthenticator**
- 5.2.2
  - 5.1.2
  - 5.0.0
  - 4.3.4
  - 4.2.1
  - 4.1.2
  - 4.0.1

**Virtualization**

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2002 and 2016
- OpenSource XenServer 4.2.5
- VMware ESXi versions 5.0, 5.5, 6.0, 6.5 and 6.7



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	✓		✓	
FortiAuthenticator	✓			
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	✓
High Availability	✓

## Language support

The following table lists FortiAnalyzer language support information.

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

Language	GUI	Reports
Russian		✓
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 create your own language translation files for these languages and import the language translation files into FortiAnalyzer by 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 about commands, 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 5.6.7. 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
<p><b>FortiGate:</b> 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,</p> <p><b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D</p> <p><b>FortiGate DC:</b> 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</p> <p><b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC</p> <p><b>Note:</b> All license-based LENC is supported based on the FortiGate support list.</p> <p><b>FortiWiFi:</b> 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</p> <p><b>FortiGate VM:</b> 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</p> <p><b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D</p> <p><b>FortiManager:</b> FMG-200D, FMG-200F, FMG-300D, FMG-300E, FMG-400E, FMG-1000D, FMG-2000E, FMG-3000F, FMG-3900E, FMG-4000D, and FMG-4000E FMG-VM64, FMG-VM64-AWS, FMG-VM64-Azure, FMG-VM64-HV (including Hyper-V 2016), FMG-VM64-KVM, and FMG-VM64-XEN (for both Citrix and Open Source Xen).</p>	5.6

Model	Firmware Version
<p><b>FortiGate:</b> 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</p> <p><b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D, FG-5001E, FG-5001E1</p> <p><b>FortiGate 6000 Series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p><b>FortiGate 7000 Series:</b> 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</p> <p><b>FortiGate DC:</b> 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</p> <p><b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC</p> <p><b>Note:</b> All license-based LENC is supported based on the FortiGate support list.</p> <p><b>FortiWiFi:</b> 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</p> <p><b>FortiGate VM:</b> 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</p> <p><b>FortiGate Rugged:</b> FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D</p>	5.4

Model	Firmware Version
<p><b>FortiGate:</b> 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</p> <p><b>FortiGate 5000 Series:</b> 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><b>FortiGate DC:</b> 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, FG-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3815D-DC, FG-3950B-DC, FG-3951B-DC</p> <p><b>FortiGate Low Encryption:</b> 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><b>FortiWiFi:</b> 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><b>FortiGate Rugged:</b> FGR-60D, FGR-100C</p> <p><b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-AWSONDEMAND, FG-VM-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN</p> <p><b>FortiSwitch:</b> FS-5203B, FCT-5902D</p>	5.2

### FortiCarrier Models

Model	Firmware Version
<p><b>FortiCarrier:</b> 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</p> <p><b>FortiCarrier DC:</b> FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C-DC, FCR-3600C-DC, FCR-3700D-DC, FCR-3810D-DC, FCR-3815D-DC</p> <p><b>FortiCarrier VM:</b> FCR-VM, FCR-VM64, FCR-VM64-AWS, FCR-VM64-AWSONDEMAND, FCR-VM64-HV, FCR-VM64-KVM</p>	5.4

Model	Firmware Version
<b>FortiCarrier:</b> 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 <b>FortiCarrier DC:</b> FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3700D-DC, FCR-3810D-DC <b>FortiCarrier Low Encryption:</b> FCR-5001A-DW-LENC <b>FortiCarrier VM:</b> FCR-VM, FCR-VM64, FCR-VM64-HV, FCR-VM64-KVM, FCR-Vm64-XEN, FCR-VM64-AWSONDEMAND	5.2

### FortiDDoS models

Model	Firmware Version
<b>FortiDDoS:</b> 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
<b>FortiAnalyzer:</b> 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. <b>FortiAnalyzer VM:</b> 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
<b>FortiAnalyzer:</b> 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. <b>FortiAnalyzer VM:</b> 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
<b>FortiAnalyzer:</b> 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 <b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
<b>FortiAnalyzer:</b> 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 <b>FortiAnalyzer VM:</b> 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
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E <b>FortiMail Low Encryption:</b> FE-3000C-LENC	5.4.5
<b>FortiMail:</b> 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 <b>FortiMail Low Encryption:</b> FE-3000C-LENC <b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3.12
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B <b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2.10
<b>FortiMail:</b> FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B <b>FortiMail VM:</b> FE-VM64	5.1.7
<b>FortiMail:</b> 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 <b>FortiMail VM:</b> FE-VM64	5.0.10

**FortiSandbox models**

Model	Firmware Version
<b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-KVM, FSA-VM	2.5.2
<b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-VM	2.4.1 2.3.3
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D, FSA-3500D <b>FortiSandbox VM:</b> FSA-VM	2.2.2 2.1.3
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D <b>FortiSandbox VM:</b> FSA-VM	2.0.3 1.4.2
<b>FortiSandbox:</b> 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
<b>FortiController:</b> FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-59	5.2.0

Model	Firmware Version
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B <b>FortiController:</b> FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B	4.3.0 4.2.0

### FortiWeb models

Model	Firmware Version
<b>FortiWeb:</b> FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D <b>FortiWeb VM:</b> FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.9.1
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D <b>FortiWeb VM:</b> FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.8.6
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D <b>FortiWeb VM:</b> FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7.2
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D <b>FortiWeb VM:</b> FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6.1
<b>FortiWeb:</b> 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	5.5.6
<b>FortiWeb VM:</b> FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE	
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E	5.4.1
<b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV	

Model	Firmware Version
<b>FortiWeb:</b> 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  <b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVEN, and FWB-HYPERV	5.3.9
<b>FortiWeb:</b> 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  <b>FortiWeb VM:</b> FWB-VM64, FWB-HYPERV, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVEN	5.2.4

### FortiCache models

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

### FortiProxy models

Model	Firmware Version
<b>FortiProxy:</b> FPX-400E, FPX-2000E  <b>FortiProxy VM:</b> FPX-KVM, FPX-VM64	1.0

# Resolved Issues

The following issues have been fixed in FortiAnalyzer version 5.6.7. For inquiries about a particular bug, please contact [Customer Service & Support](#).

## FortiView

Bug ID	Description
518346	Export to report sticks at 5% after drill down under Top Browsing Users.

## Log View

Bug ID	Description
516098	Real time view for all devices does not show any data and return no records found.

## Reports

Bug ID	Description
510401	Date format change is not applied to Chart when type is selected as Area or Line.
515762	Drill-down Resource Usage Details report only provides details up to first two days of the reporting period.

## System Settings

Bug ID	Description
404298	The free-text filter for log forwarding does not work on syslog that does not follow a specific format.
508102	Log forwarded from FortiAnalyzer no longer includes time zone causing compatibility issues with other Fortinet products.
516205	The filter for log forwarding is not working well when there is message with multiple logs.



Bug ID	Description
517724	The System Resources widget may not show correct outputs.

## Others

Bug ID	Description
512413	Malformed compact v3 log may cause daemon to crash due to log parsing error.
515988	Parameters for storage usage do not change in CLI after they are modified from GUI.
502046	FortiAnalyzer stop responding to GUI access and many services are in Z state.

## Common Vulnerabilities and Exposures

Visit <https://fortiguard.com/psirt> for more information.

Bug ID	Description
464795	FortiAnalyzer 5.6.7 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2017-17541</li></ul>
473644	FortiAnalyzer5.6.7 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2018-1354</li></ul>
474994	FortiAnalyzer 5.6.7 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2018-1355</li></ul>

# Known Issues

The following issues have been identified in FortiAnalyzer version 5.6.7. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

## FortiView

Bug ID	Description
527064	After the upgrade, the BW reported for applications is 5 to 20 times higher.

## Log View

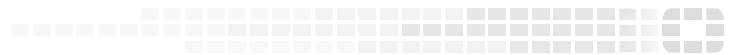
Bug ID	Description
442713	Regular searches for strings that contain a space character combined with another one returns no results.

## Others

Bug ID	Description
526943	Log forwarding to their syslog server may stop working after a few days.



**FORTINET®**



Copyright© 2018 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.