



FortiAnalyzer - Release Notes

Version 6.0.8

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 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: techdoc@fortinet.com



January 28, 2020

FortiAnalyzer 6.0.8 Release Notes

05-608-604522-20200128

TABLE OF CONTENTS

Change Log	5
FortiAnalyzer 6.0.8 Release	6
Supported models	6
Special Notices	7
Port 8443 reserved	7
FortiManager features disabled when FortiAnalyzer HA enabled	7
Updated Widgets for Fortinet Security Fabric	7
Hyper-V FortiAnalyzer-VM running on an AMD CPU	7
SSLv3 on FortiAnalyzer-VM64-AWS	7
Pre-processing logic of eptime	8
Upgrade Information	9
Upgrading to FortiAnalyzer 6.0.x	9
Downgrading to previous versions	9
Firmware image checksums	9
FortiAnalyzer VM firmware	10
SNMP MIB files	11
Product Integration and Support	12
FortiAnalyzer version 6.0.8 support	12
Web browsers	12
FortiOS/FortiOS Carrier	13
FortiAnalyzer	13
FortiAuthenticator	13
FortiCache	13
FortiClient	14
FortiDDoS	14
FortiMail	14
FortiManager	14
FortiSandbox	14
FortiSwitch ATCA	14
FortiWeb	15
Virtualization	15
Feature support	15
FortiGate Management	16
Language support	16
Supported models	17
FortiGate models	18
FortiCarrier models	21
FortiDDoS models	21
FortiAnalyzer models	22
FortiMail models	22
FortiSandbox models	23
FortiSwitch ATCA models	24
FortiWeb models	24

FortiCache models	25
FortiProxy models	25
FortiAuthenticator models	26
Resolved Issues	27
Event Management	27
FortiView	27
Log View	27
Others	27
Reports	28
System Settings	28
Known Issues	29
Device Manager	29
Log View	29
Others	29
Reports	30

Change Log

Date	Change Description
2020-01-22	Initial release of 6.0.8.
2020-01-28	Updated FortiOS/FortiOS Carrier on page 13

FortiAnalyzer 6.0.8 Release

This document provides information about FortiAnalyzer version 6.0.8 build 0429.



The recommended minimum screen resolution for the FortiAnalyzer GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:

- [Supported models on page 6](#)

Supported models

FortiAnalyzer version 6.0.8 supports the following models:

FortiAnalyzer	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.
FortiAnalyzer VM	FAZ-VM64, FAZ-VM64-ALI, 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).

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer version 6.0.8.

Port 8443 reserved

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

FortiManager features disabled when FortiAnalyzer HA enabled

If you have FortiManager features enabled on FortiAnalyzer units, and then enable HA for the FortiAnalyzer units, FortiManager features are automatically disabled. FortiManager features are not supported when FortiAnalyzer HA is enabled.

Updated Widgets for Fortinet Security Fabric

After upgrading FortiAnalyzer from 5.6 to 6.0, the NOC Security Fabric widgets, *Security Fabric Score Summary* and *Historical Security Fabric Scores*, no longer show any data. These two widgets have been replaced by the following widgets: *Security Fabric Rating Report* and *Security Fabric Scores* in FortiAnalyzer 6.0. The two new widgets only support FortiOS 6.0 devices.

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.

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.

Upgrade Information

You can upgrade FortiAnalyzer 5.6.0 or later directly to 6.0.8.



For other upgrade paths and details about upgrading your FortiAnalyzer, see *FortiAnalyzer Upgrade Guide* in the Document Library.

Upgrading to FortiAnalyzer 6.0.x

Upgrading to FortiAnalyzer 6.0.x automatically triggers an SQL database rebuild, which must complete for FortiAnalyzer to function normally. Verify the database rebuild status using `diagnose sql status rebuild-db`.

This section contains the following topics:

- [Downgrading to previous versions on page 9](#)
- [Firmware image checksums on page 9](#)
- [FortiAnalyzer VM firmware on page 10](#)
- [SNMP MIB files on page 11](#)

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.

Aliyun

- `.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.

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 FortiAnalyzer VM installation.
- `.out.gcp.zip`: Download the 64-bit package for a new FortiAnalyzer 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

This section lists FortiAnalyzer 6.0.8 support of other Fortinet products. It also identifies what FortiAnalyzer features are supported for log devices, what FortiGate management features are supported when FortiManager features are enabled on FortiAnalyzer, and what languages FortiAnalyzer GUI and reports support. It also lists which Fortinet models can send logs to FortiAnalyzer.

The section contains the following topics:

- [FortiAnalyzer version 6.0.8 support on page 12](#)
- [Feature support on page 15](#)
- [FortiGate Management on page 16](#)
- [Language support on page 16](#)
- [Supported models on page 17](#)

FortiAnalyzer version 6.0.8 support

This section identifies FortiAnalyzer version 6.0.8 product integration and support information:

- [Web browsers on page 12](#)
- [FortiOS/FortiOS Carrier on page 13](#)
- [FortiAnalyzer on page 13](#)
- [FortiAuthenticator on page 13](#)
- [FortiCache on page 13](#)
- [FortiClient on page 14](#)
- [FortiDDoS on page 14](#)
- [FortiMail on page 14](#)
- [FortiManager on page 14](#)
- [FortiSandbox on page 14](#)
- [FortiSwitch ATCA on page 14](#)
- [FortiWeb on page 15](#)
- [Virtualization on page 15](#)



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

Web browsers

This section lists FortiAnalyzer version 6.0.8 product integration and support for web browsers:

- Microsoft Edge 40
Due to limitation on Edge, the browser may not completely render a page with a large set of policies or objects.
- Mozilla Firefox version 72
- Google Chrome version 79

FortiOS/FortiOS Carrier

This section lists FortiAnalyzer version 6.0.8 product integration and support for FortiOS/FortiOS Carrier:

- 6.0.0 to 6.0.9
- 5.6.0 to 5.6.12
- 5.4.0 to 5.4.13
- 5.2.0 to 5.2.15

FortiAnalyzer

This section lists FortiAnalyzer version 6.0.8 product integration and support for FortiAnalyzer:

- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiAuthenticator

This section lists FortiAnalyzer version 6.0.8 product integration and support for FortiAuthenticator:

- 5.5.0
- 5.4.0 to 5.4.1
- 5.3.1
- 5.2.2
- 5.1.0
- 5.0.0
- 4.3.0
- 4.2.0
- 4.1.0

FortiCache

This section lists FortiAnalyzer version 6.0.8 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

FortiClient

This section lists FortiAnalyzer version 6.0.8 product integration and support for FortiClient:

- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiDDoS

This section lists FortiAnalyzer version 6.0.8 product integration and support for FortiDDoS:

- 4.6.0
- 4.4.2
- 4.2.3

FortiMail

This section lists FortiAnalyzer version 6.0.8 product integration and support for FortiMail:

- 6.0.7
- 5.4.10
- 5.3.12

FortiManager

This section lists FortiAnalyzer version 6.0.8 product integration and support for FortiManager:

- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiSandbox

This section lists FortiAnalyzer version 6.0.8 product integration and support for FortiSandbox:

- 3.0.0 to 3.0.5
- 2.5.0 to 2.5.2
- 2.4.0 and 2.4.1
- 2.3.2 and 2.3.3
- 2.2.2

FortiSwitch ATCA

This section lists FortiAnalyzer version 6.0.8 product integration and support for FortiSwitch ATCA:

- 5.0.0 and later

FortiWeb

This section lists FortiAnalyzer version 6.0.8 product integration and support for FortiWeb:

- 6.0.7
- 5.9.1
- 5.8.6
- 5.7.2
- 5.6.1
- 5.5.6
- 5.4.1

Virtualization

This section lists FortiAnalyzer version 6.0.8 product integration and support for virtualization:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012 and 2016
- OpenSource XenServer 4.2.5
- VMware ESXi versions 5.0, 5.5, 6.0, 6.5 and 6.7

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	✓		✓	✓

Platform	Log View	FortiView	Event Management	Reports
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.



FortiAnalyzer HA is not supported when FortiManager features are enabled.

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	
FortiManager HA	
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		✓
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 by exporting a predefined language from FortiManager, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiManager. For more information, see the *FortiAnalyzer Administration Guide*.

Supported models

This section identifies which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch, FortiWeb, FortiCache, and FortiProxy models and firmware versions can send logs to a FortiAnalyzer appliance running version 6.0.8. 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.

This section contains the following topics:

- [FortiGate models on page 18](#)
- [FortiCarrier models on page 21](#)
- [FortiDDoS models on page 21](#)
- [FortiAnalyzer models on page 22](#)
- [FortiMail models on page 22](#)
- [FortiSandbox models on page 23](#)
- [FortiSwitch ATCA models on page 24](#)
- [FortiWeb models on page 24](#)

- [FortiCache models on page 25](#)
- [FortiProxy models on page 25](#)
- [FortiAuthenticator models on page 26](#)

FortiGate models

Model	Firmware Version
<p>FortiGate: FGT-30E-3G4G-GBL, FGT-60F, FGT-61F, FGT-3400E, FGT-3401E, FGT-3600E, FGT-3601E, FGT-400E, FGT-401E, FGT-600E, FGT-601E, FGT-60E-DSL, FGT-60E-DSLJ, FWF-60E-DSL, FWF-60E-DSLJ, FGT-VM64-RAXONDEMAND, FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, 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-100F, FG-101F, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3600C, FG3700D, FG-3800D, FG-3810D, FG-3815D, FG-1100E, FG-1101E, FG-2200E, FG-2201E, FG-3300E, FG-3301E, FG-3960E, FG-3980E, FG-6000F</p> <p>FortiGate 5000 Series: FG-5001D, FG-5001E, FG-5001E1</p> <p>FortiGate 6000 Series: FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p>FortiGate 7000 Series: FG-7030E-S, FG-7030E-Q, 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-7040E-9-DC, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6, FG-7060E-8, FG-7060E-9, FortiGate-7060E-8-DC</p> <p>FortiGate DC: FG-800D-DC, FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC</p> <p>FortiGate Hardware Low Encryption: FG-100D-LENC,</p> <p>Note: All license-based LENC is supported based on the FortiGate support list.</p> <p>FortiWiFi: FWF-30D, 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-90D, FWF-90D-POE, FWF-92D</p> <p>FortiGate VM: FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen</p> <p>FortiGate Rugged: FGR-30D, FGR-35D, FGR-60D, FGR-90D</p>	6.0

Model	Firmware Version
<p>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-60E-DSL, 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-100F, 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>FortiGate 5000 Series: FG-5001C, FG-5001D, FG-5001E, FG-5001E1</p> <p>FortiGate 6000 Series: FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p>FortiGate 7000 Series: FG-7030E, FG-7040E, FG-7060E</p> <p>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, FG-7060E-8-DC</p> <p>FortiGate Hardware Low Encryption: FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC</p> <p>Note: All license-based LENC is supported based on the FortiGate support list.</p> <p>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</p> <p>FortiGate VM: FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-Azure, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOSVM64, FOSVM64-KVM, FOS-VM64-Xen</p> <p>FortiGate Rugged: FGR-30D, FGR-35D, FGR-60D, FGR-90D</p>	5.6
<p>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-100F, 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>FortiGate 5000 Series: FG-5001C, FG-5001D, FG-5001E, FG-5001E1</p> <p>FortiGate 6000 Series: FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p>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</p> <p>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, FG-7060E-8-DC</p>	5.4

Model	Firmware Version
<p>FortiGate Hardware Low Encryption: FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC</p> <p>Note: All license-based LENC is supported based on the FortiGate support list.</p> <p>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</p> <p>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</p> <p>FortiGate Rugged: FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D</p>	
<p>FortiGate: FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600C, FG-600D, FG-620B, FG-621B, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-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>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-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>FortiGate Low Encryption: FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC</p> <p>FortiWiFi: FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D</p> <p>FortiGate Rugged: FGR-60D, FGR-100C</p> <p>FortiGate VM: FG-VM, FG-VM64, FG-VM64-AWSONDEMAND, FG-VM-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN</p> <p>FortiSwitch: FS-5203B, FCT-5902D</p>	5.2

FortiCarrier models

Model	Firmware Version
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E FortiCarrier-DC: FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC FortiCarrier-VM: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	6.0
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001C, FGT-5001D, FGT-5001E FortiCarrier 6000 Series: FG-6300F, FG-6301F, FG-6500F, FG-6501F FortiCarrier 7000 Series: FG-7030E, FG-7040E, FG-7060E FortiCarrier-DC: FGT-3000D-DC, FGC-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FCR-3810D-DC, FCR-7060E-8-DC FortiCarrier-VM: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	5.6
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-5001C, FGT-5001D, FGT-7030E, FGT-7040E FortiCarrier 6000 Series: FG-6300F, FG-6301F, FG-6500F, FG-6501F FortiCarrier 7000 Series: FG-7030E, FG-7040E, FG-7060E FortiCarrier-DC: FGT-3000D-DC, FGC-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FCR-7060E-8-DC FortiCarrier-VM: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	5.4
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, , FGT-3810A, FGT-3810D, FGT-3950B, FGT-3951B, FGT-5100B, FGT-5100C, FGT-5001D, FGT-5101C, FS-5203B, FT-5902D FortiCarrier-DC: FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3810A-DC, FGT-3810D-DC, FGT-3950B-DC, FGT-3951B-DC FortiCarrier-VM: FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-Xen	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-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, 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)	6.0
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-800F, 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-800F, 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-800F, 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-800F, 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-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E FortiMail VM: FE-VM64	6.0
FortiMail: FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E FortiMail Low Encryption: FE-3000C-LENC	5.4.6 5.4.2

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	5.3.12
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	5.2.10
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	5.1.7
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-KVM, FSA-VM	3.0.1
	3.0.0
	2.5.2
	2.5.1
	2.5.0
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox VM: FSA-VM	2.4.1
	2.4.0
	2.3.3
	2.3.2
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D FortiSandbox VM: FSA-VM	2.2.2
	2.1.3
FortiSandbox: FSA-1000D, FSA-3000D FortiSandbox VM: FSA-VM	2.0.3
	1.4.2
FortiSandbox: FSA-1000D, FSA-3000D	1.4.0 and 1.4.1
	1.3.0
	1.2.0 and later

FortiSwitch ATCA 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-100D, FWB-400C, FWB-400D, FWB-600D, FWB-1000D, FWB-1000E, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E FortiWeb VM: FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVEN	6.0.1
FortiWeb: 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 FortiWeb VM: 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
FortiWeb: 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 FortiWeb VM: 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
FortiWeb: 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 FortiWeb VM: FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7.2
FortiWeb: 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 FortiWeb VM: FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6.1

Model	Firmware Version
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-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.6
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-XENSERVR, 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-XENSERVR, and FWB-HYPERV	5.3.9
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-XENSERVR	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

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E FortiProxy VM: FPX-KVM, FPX-VM64	1.0

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E	5.5.0
FortiAuthenticator VM: FAC-VM, FAC-VM-HV, FAC-VM-KVM, FAC-VM-XEN	

Resolved Issues

The following issues have been fixed in FortiAnalyzer version 6.0.8. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Event Management

Bug ID	Description
563514	Event handler does not work properly for FortiSandbox.

FortiView

Bug ID	Description
562834	On FortiView > Top Sources, FortiAnalyzer displays incorrect data when trying to filter logs with Source and User.
574836	FortiAnalyzer may not be able to show the Compromised Hosts.
574998	FortiAnalyzer may not be able to show new logs under FortiView.
581158	Sorting by Threat Score in descending order should display entries with most Threat Score first.

Log View

Bug ID	Description
573281	Unregistered syslog device appears with FortiMail's IP after added FortiMail device.

Others

Bug ID	Description
601383	FortiAnalyzer may become unresponsive when source IPs change often for all endpoints due to DHCP.

Bug ID	Description
544516	FortiAnalyzer with Hyper-V live migration blocks access to GUI.
588074	FortiAnalyzer may stop receiving logs and event logs, and continuously display oftpd re-initialization.
590368	FortiAnalyzer may stop receiving logs after oftpd crashed.
596252	The clustered daemon may consume high CPU resource.

Reports

Bug ID	Description
552414	Read-write permissions are required to view and download reports through API call.
589496	FortiAnalyzer may generate a different result when running a report on the same time period either with a custom time period or a specific time period from the dropdown list.

System Settings

Bug ID	Description
565200	FortiAnalyzer may show incorrect Available Disk space status under storage information.
571412	Logging topology is misleading when collector mode in FortiAnalyzer is deployed.
590109	Some time zone are not formatted correctly when forwarding as syslog.
600639	FortiAnalyzer may not be able to move a VDOM with a long name from the Root ADOM to another ADOM.

Known Issues

The following issues have been identified in FortiAnalyzer version 6.0.8. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Device Manager

Bug ID	Description
596832	FortiGate Cluster is removed from log forwarding on failover when FortiAnalyzer is managed by a FortiManager.

Log View

Bug ID	Description
550523	Downloading logs from Log View randomly fails.
579871	Restoration of logs does not show correct timestamps under log browse after a NTP out of sync event.
591841	There may be a delay for FortiAnalyzer to show Historical Logs.
597192	Downloading logs may take longer than log search.

Others

Bug ID	Description
587489	Analytic data may be removed due to high disk usage.
592593	FortiAnalyzer may update ADOM disk allocation or create ADOM without any checks when request is made via JSON API.

Reports

Bug ID	Description
547496	FortiAnalyzer generates a report for selected device with outputs for all devices.
553495	FortiAnalyzer may prompt Web Server 404 Error when trying to download Report with 100,000 lines.
557388	There are discrepancies in Bandwidth and Applications Report for predefined data sets on the same report time period.
558084	FortiAnalyzer should not generate logs stating "Can not find user:admin when running report: 1000060025".



FORTINET[®]



Copyright© 2020 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.