



FortiAnalyzer - Release Notes

Version 6.4.2

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



April 12, 2021

FortiAnalyzer 6.4.2 Release Notes

05-642-651940-20210412

TABLE OF CONTENTS

Change Log	5
FortiAnalyzer 6.4.2 Release	6
Supported models	6
FortiAnalyzer VM subscription license	6
FortiRecorder	7
Supported models for FortiRecorder	7
Supported cameras	7
Special Notices	8
Citrix XenServer default limits and upgrade	8
FortiAnalyzer Cloud VM does not support FortiGate 6.4.0	8
FortiAnalyzer VM upgrade requires more memory	8
Maximum ADOM limits for FortiAnalyzer	9
Port 8443 reserved	9
All OFTP connections must be encrypted for FortiAnalyzer 6.2.0 (or higher)	9
Hyper-V FortiAnalyzer-VM running on an AMD CPU	9
SSLv3 on FortiAnalyzer-VM64-AWS	9
Upgrade Information	10
Downgrading to previous versions	10
Firmware image checksums	10
FortiAnalyzer VM firmware	10
SNMP MIB files	12
Product Integration and Support	13
FortiAnalyzer version 6.4.2 support	13
Web browsers	13
FortiOS/FortiOS Carrier	14
FortiAnalyzer	14
FortiAuthenticator	14
FortiCache	14
FortiClient	14
FortiDDoS	15
FortiMail	15
FortiManager	15
FortiProxy	15
FortiSandbox	16
FortiSwitch ATCA	16
FortiWeb	16
Virtualization	16
Feature support	17
Language support	17
Supported models	18
FortiGate models	19
FortiCarrier models	22
FortiDDoS models	23

FortiAnalyzer models	24
FortiMail models	25
FortiSandbox models	25
FortiSwitch ATCA models	26
FortiWeb models	26
FortiCache models	28
FortiProxy models	28
FortiAuthenticator models	28
Resolved Issues	29
Device Manager	29
FortiView	29
Log View	29
Others	30
Reports	30
System Settings	30
Common Vulnerabilities and Exposures	30
Known Issues	32
Device Manager	32
Event Management	32
FortiView	32
FortiSoC	33
Log View	33
Others	34
Reports	35
System Settings	35
Appendix A - Recommended maximum number of ADOMs supported	37

Change Log

Date	Change Description
2020-08-06	Initial release of 6.4.2.
2020-08-17	Updated FortiClient on page 14.
2020-09-10	Updated Known Issues on page 32.
2020-09-16	Updated FortiOS/FortiOS Carrier on page 14.
2020-09-17	Updated Known Issues on page 32 and Resolved Issues on page 29
2020-10-15	Updated Virtualization on page 16.
2020-11-04	Updated FortiGate models on page 19.
2021-01-04	Updated Supported models on page 6.
2021-02-04	Updated Supported models on page 6.
2021-02-23	Updated Virtualization on page 16.
2021-04-12	Added FortiAnalyzer VM subscription license on page 6.

FortiAnalyzer 6.4.2 Release

This document provides information about FortiAnalyzer version 6.4.2 build 2122.



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](#)
- [FortiAnalyzer VM subscription license on page 6](#)
- [FortiRecorder on page 7](#)

Supported models

FortiAnalyzer version 6.4.2 supports the following models:

FortiAnalyzer	FAZ-200F, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000E, FAZ-2000E, FAZ-3000E, FAZ-1000F, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3500G, 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).

FortiAnalyzer VM subscription license

The FortiAnalyzer VM subscription license supports FortiAnalyzer version 6.4.1 and later. For information about supported firmware, see [FortiAnalyzer VM firmware on page 10](#).

See also [Appendix A - Recommended maximum number of ADOMs supported on page 37](#).



You can use the FortiAnalyzer VM subscription license with new FAZ-VM installations. For existing FAZ-VM installations, you cannot upgrade to a FortiAnalyzer VM subscription license. Instead, you must migrate data from the existing FAZ-VM to a new FAZ-VM with subscription license.

FortiRecorder

This section identifies what FortiAnalyzer models support the FortiRecorder module and what FortiCamera models are supported.

Supported models for FortiRecorder

Below is a list of the FortiAnalyzer appliances that support the FortiRecorder module.

Platform	Maximum number of cameras
FAZ-200F	4
FAZ-300F	6
FAZ-400E	12
FAZ-800F	16
FAZ-1000E	30
FAZ-1000F	50
FAZ-2000E	40
FAZ-3000F	50
FAZ-3700F	60
FAZ-3500G	50

Supported cameras

The following FortiCamera models are supported in the FortiRecorder module:

- FCM-CB20
- FCM-FD20
- FCM-FD20B
- FCM-FD40
- FCM-MB40
- FCM-MD20
- FCM-MD40
- FCM-OB30

Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer version 6.4.2.

Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FAZ-VM64-XEN image is larger than 128M. Before updating to FortiAnalyzer 6.4, increase the size of the ramdisk setting on Citrix XenServer.

To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:

```
xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912
```
2. Confirm the setting is in effect by running `xenstore-ls`.

```
limits = ""  
pv-kernel-max-size = "33554432"  
pv-ramdisk-max-size = "536,870,912"  
boot-time = ""
```

3. Remove the pending files left in `/run/xen/pygrub`.



The ramdisk setting returns to the default value after rebooting.

FortiAnalyzer Cloud VM does not support FortiGate 6.4.0

FortiManager and FortiAnalyzer Cloud VMs do not currently support FortiGate 6.4.0. Cloud VM users should continue using FortiGate firmware 6.2 builds. Cloud platforms will be supported in a future 6.4 patch release.

FortiAnalyzer VM upgrade requires more memory

When upgrading FortiAnalyzer VM units from FortiAnalyzer 6.2.x to FortiAnalyzer 6.4.0 and later, the upgrade may fail because of memory allocation.

Workaround: Before upgrading FortiAnalyzer VM to FortiAnalyzer 6.4.0 and later, change the memory allocation to 8 GB of RAM.

Maximum ADOM limits for FortiAnalyzer

FortiAnalyzer hardware devices and VMs display a warning when the maximum number of ADOMs is reached or exceeded. The platform does not enforce the limit; however, adding more ADOMs may affect the performance of the unit. For more details, see [Appendix A - Recommended maximum number of ADOMs supported on page 37](#).

Port 8443 reserved

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

All OFTP connections must be encrypted for FortiAnalyzer 6.2.0 (or higher)

Prior to upgrading to FortiAnalyzer 6.2, make sure that all FortiGate devices are configured to use encryption when communicating with FortiAnalyzer. Starting with FortiAnalyzer 6.2.0, all OFTP communications must be encrypted.

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
```

Upgrade Information

You can upgrade FortiAnalyzer 6.2.0 or later directly to 6.4.2.



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

This section contains the following topics:

- [Downgrading to previous versions on page 10](#)
- [Firmware image checksums on page 10](#)
- [FortiAnalyzer VM firmware on page 10](#)
- [SNMP MIB files on page 12](#)

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.

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 FortiAnalyzer product data sheet available on the Fortinet web site, <https://www.fortinet.com/products/management/fortianalyzer.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 6.4.2 support of other Fortinet products. It also identifies what FortiAnalyzer features are supported for log devices 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 6.4.2 support on page 13](#)
- [Feature support on page 17](#)
- [Language support on page 17](#)
- [Supported models on page 18](#)

FortiAnalyzer version 6.4.2 support

This section identifies FortiAnalyzer version 6.4.2 product integration and support information:

- [Web browsers on page 13](#)
- [FortiOS/FortiOS Carrier on page 14](#)
- [FortiAnalyzer on page 14](#)
- [FortiAuthenticator on page 14](#)
- [FortiCache on page 14](#)
- [FortiClient on page 14](#)
- [FortiDDoS on page 15](#)
- [FortiMail on page 15](#)
- [FortiManager on page 15](#)
- [FortiProxy on page 15](#)
- [FortiSandbox on page 16](#)
- [FortiSwitch ATCA on page 16](#)
- [FortiWeb on page 16](#)
- [Virtualization on page 16](#)



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

Web browsers

This section lists FortiAnalyzer version 6.4.2 product integration and support for web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 79

- Google Chrome version 84

FortiOS/FortiOS Carrier

This section lists FortiAnalyzer version 6.4.2 product integration and support for FortiOS/FortiOS Carrier:

- 6.4.0 and later
- 6.2.0 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiAnalyzer

This section lists FortiAnalyzer version 6.4.2 product integration and support for FortiAnalyzer:

- 6.4.0 to 6.4.2
- 6.2.0 to 6.2.2
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiAuthenticator

This section lists FortiAnalyzer version 6.4.2 product integration and support for FortiAuthenticator:

- 6.0.0 and later
- 5.0 to 5.5
- 4.3.0 and later

FortiCache

This section lists FortiAnalyzer version 6.4.2 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

FortiClient

This section lists FortiAnalyzer version 6.4.2 product integration and support for FortiClient:

- 6.4.0 and later
- 6.2.7
- 6.0.9

- 5.6.6
- 5.4.0 and later

FortiDDoS

This section lists FortiAnalyzer version 6.4.2 product integration and support for FortiDDoS:

- 5.3.0
- 5.2.0
- 5.1.0
- 5.0.0
- 4.7.0
- 4.6.0
- 4.5.0
- 4.4.2
- 4.3.2
- 4.2.3

FortiMail

This section lists FortiAnalyzer version 6.4.2 product integration and support for FortiMail:

- 6.4.0
- 6.2.4
- 6.0.9
- 5.4.11
- 5.3.13

FortiManager

This section lists FortiAnalyzer version 6.4.2 product integration and support for FortiManager:

- 6.4.0 and later
- 6.2.0 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiProxy

This section lists FortiAnalyzer version 6.4.2 product integration and support for FortiProxy:

- 1.0

FortiSandbox

This section lists FortiAnalyzer version 6.4.2 product integration and support for FortiSandbox:

- 3.1.2
- 3.0.6
- 2.5.2
- 2.4.1
- 2.3.3
- 2.2.2

FortiSwitch ATCA

This section lists FortiAnalyzer version 6.4.2 product integration and support for FortiSwitch ATCA:

- 5.0.0 and later

FortiWeb

This section lists FortiAnalyzer version 6.4.2 product integration and support for FortiWeb:

- 6.3.2
- 6.2.3
- 6.1.2
- 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 6.4.2 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
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5
- VMware ESXi versions 5.0, 5.5, 6.0, 6.5, 6.7, and 7.0

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	✓		✓	
FortiProxy	✓		✓	✓
FortiSandbox	✓		✓	✓
FortiWeb	✓		✓	✓
Syslog	✓		✓	✓

Language support

The following table lists FortiAnalyzer language support information.

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

Language	GUI	Reports
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 FortiAnalyzer, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiAnalyzer. 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 6.4.2. 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 19](#)
- [FortiCarrier models on page 22](#)
- [FortiDDoS models on page 23](#)
- [FortiAnalyzer models on page 24](#)
- [FortiMail models on page 25](#)
- [FortiSandbox models on page 25](#)
- [FortiSwitch ATCA models on page 26](#)
- [FortiWeb models on page 26](#)
- [FortiCache models on page 28](#)
- [FortiProxy models on page 28](#)
- [FortiAuthenticator models on page 28](#)

FortiGate models

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3301E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 FortiGate DC: FortiGate-800D-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC FortiGate Hardware Low Encryption: FortiGate-100D-LENC FortiWiFi: FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61F FortiGate VM: FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM FortiOS: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	6.4
FortiGate: FortiGate-30E, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3301E, FortiGate-3960E, FortiGate-3980E FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1	6.2

Model	Firmware Version
FortiGate DC: FortiGate-80C-DC, FortiGate-600C-DC, FortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3600C-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC FortiGate Hardware Low Encryption: FortiGate-80C-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC FortiWiFi: FortiWiFi-30D, FortiWiFi-30D-POE, FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61F, FortiWiFi-80CM, FortiWiFi-81CM FortiGate-VM: FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager FortiGate Rugged: FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D FortiOS: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-GBL, 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-DSLJ, FG-60E-POE, FG-40F, FG-40F-3G4G, FG-60F, FG-61F, 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-100EF, FG-101E, FG-100F, FG-101F, 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, 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, FortiGate-2200E, FortiGate-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301EFG-3600C, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FortiGate-3301E, FG-3960E, FG-3980E FortiGate 5000 Series: FG-5001D, FG-5001E, FG-5001E1 FortiGate DC: FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC FortiGate Hardware Low Encryption: FG-100D-LENC, FG-600C-LENC Note: All license-based LENC is supported based on the FortiGate support list. 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, FortiWiFi-60F, FortiWiFi-61F, FWF-90D, FWF-90D-POE, FWF-92D FortiGate VM: FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP, 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 FortiGate Rugged: FGR-30D, FGR-35D, FGR-60D, FGR-90D	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-DSLJ, 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-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p>FortiGate 7000 Series: FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC</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-60E-DSL, FWF-60E-DSLJ, 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, FG-3980E, FG-2000E, FG-2500E</p> <p>FortiGate 5000 Series: FG-5001C, FG-5001D, FG-5001E, FG-5001E1</p> <p>FortiGate 6000 Series: FG-6000F, 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>	5.4

Model	Firmware Version
(Update only) FortiGate 7000 series: FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC 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 FortiGate Hardware Low Encryption: FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC Note: All license-based LENC is supported based on the FortiGate support list. 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	

FortiCarrier models

Model	Firmware Version
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3400E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 FortiCarrier-DC: FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC FortiCarrier-VM: FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 FortiCarrier-DC: FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC FortiCarrier-VM: FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.2
FortiCarrier: FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E	6.0

Model	Firmware Version
FortiGate 6000 series: FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F FortiGate 7000 series: FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC 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	
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-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F FortiCarrier 7000 Series: FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC FortiCarrier-DC: FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC, FGT-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, FG-3600E, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-5001C, FGT-5001D, FGT-7030E, FGT-7040E FortiCarrier 6000 Series: FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F FortiCarrier 7000 Series: FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC FortiCarrier-DC: FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-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

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-200B, FortiDDoS-400B, FortiDDoS-600B, FortiDDoS-800B, FortiDDoS-900B, FortiDDoS-1000B, FortiDDoS-1200B, FortiDDoS-1500E, FortiDDoS-2000B, FortiDDoS-2000E	5.2, 5.3
FortiDDoS: FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-1500B, FI-2000B, FI-2000E	5.1
FortiDDoS: FI-1500E, FI-2000E	5.0
FortiDDoS: FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.0, 4.1, 4.2, 4.3, 4.4, 4.5, 4.7

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E FortiAnalyzer VM: FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	6.4
FortiAnalyzer: FAZ-200F, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000E, FAZ-2000E, 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).	6.2
FortiAnalyzer: FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. FortiAnalyzer VM: FAZ-VM64, FAZ-VM64-AWS, FMG-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-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. FortiAnalyzer VM: FAZ-VM64, FAZ-VM64-AWS, FMG-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, FMG-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-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-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-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-200F, FML-400F, FML-900F	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
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
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
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
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

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox-VM: FSA-AWS, FSA-VM	3.1
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox VM: FSA-AWS, FSA-VM	3.0
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox VM: FSA-KVM, FSA-VM	2.5.2
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox VM: FSA-VM	2.4.1 2.3.3
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D FortiSandbox VM: FSA-VM	2.2.0 2.1.3
FortiSandbox: FSA-1000D, FSA-3000D	2.0.3 1.4.2

Model	Firmware Version
FortiSandbox VM: FSA-VM	
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	5.0.0
FortiController: FTCL-5103B, FTCL-5903C, FTCL-5913C	
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3.0 4.2.0

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E	6.2, 6.3
FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	
FortiWeb: FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E	6.1
FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XenServer	
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	6.0.1
FortiWeb VM: FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVER	
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	5.9.1

Model	Firmware Version
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	
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
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-3000E, FCH-3900E	4.0, 4.1, 4.2
FortiCache VM: FCH-VM64, FCH-KVM	

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E	1.0/1.1
FortiProxy VM: FPX-KVM, FPX-VM64	

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000B, FAC-3000D, FAC-3000E	4.3, 5.0-5.5, 6.0
FortiAuthenticator VM: FAC-VM	
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E	4.0-4.2
FortiAuthenticator VM: FAC-VM	

Resolved Issues

The following issues have been fixed in FortiAnalyzer version 6.4.2. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Device Manager

Bug ID	Description
641490	FortiAnalyzer may fail to update HA group name after the group name is changed on the FortiGate side causing it crash occasionally.
648893	Device list may be empty in <i>Device Manager</i> after upgrade.

FortiView

Bug ID	Description
590775	FortiAnalyzer should hide <i>Device</i> and <i>Time Frame</i> selection in <i>FortiView Threat Map</i> .
624856	Default user filter is missing from <i>FortiView > VPN > SSL & Dialup IPsec</i> in filter mode while it is available in text mode.
632532	Drill-down in FortiView does not display correctly when log is at the bottom of the display.
641616	Exporting chart from FortiView triggers both successful and error messages.
641983	Traffic filter by policy ID with greater or less than option is not working correctly when viewing real-time logs.

Log View

Bug ID	Description
636967	After upgrade, FortiAnalyzer reports problem that filter in real-time log does not work resulting in <i>No entry found</i> .
642960	Logs imported in <i>Log Browse</i> may not show up in traffic logs.

Others

Bug ID	Description
630900	FortiAnalyzer should add filters from session-view to default skip-index list.
645965	The <code>diagnose dvm device list</code> command shows incorrect VDOM to ADOM assignment and Fabric view Asset displays data belonging to different ADOMs.
647589	EMS sysinfo wildcard call should be <code>{'uid_list': []}</code> instead of <code>{'uid_list': ['']}</code> .
644232	FortiAnalyzer may use high IO usage on VACUUM process.
652541	The <code>siemagentd</code> may hang under load.

Reports

Bug ID	Description
296148	FortiAnalyzer needs to restrict log tables when creating a view for dataset testing.
528395	Deleting device from Device Manager removes the report filter but does not stop schedule and notifications.
643238	User should be able filter reports based on device name in <i>Reports > Report Definitions > All Reports</i> .

System Settings

Bug ID	Description
599771	When logging in with an LDAP admin, one invalid ADOM value may cause 'authentication failed'.
613032	Cover page files may be not synchronized to secondary unit.
642459	Syslogd receives empty logs when FortiAnalyzer forwards FortiExtender logs.
644863	When SAML uses Supper_User under root ADOM, the user is not able to view analytic logs under FortiView and Event handler prompts "Web Server Error 500".

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
626913	FortiAnalyzer 6.4.2 is no longer vulnerable to the following CVE-Reference: <ul style="list-style-type: none">• CVE-2020-12817

Known Issues

The following issues have been identified in FortiAnalyzer version 6.4.2. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Device Manager

Bug ID	Description
613115	Device Manager view may show red icons for VDOMs even when logs are received.
517643	When manually adding a device to a Fabric ADOM, FortiAnalyzer should not display Firmware Version.
523721	FortiAnalyzer should support FortiADC device type.
573684	When EMS is configured to send logs to FortiAnalyzer, EMS IP address is always 0.0.0.0.
639479	FortiGate v6.0 with sub-ca certificate may not be able to establish <code>oftp</code> connection with FortiAnalyzer without sub-ca certificate.
651696	<i>Device Manager > Device > Average Log Rate (Logs/Sec)</i> sort function does not work.

Event Management

Bug ID	Description
632326	Syslog type <i>Event Handler Alert</i> sends an Email that is truncated.
638676	SNMP alert is not generated for event handler is triggered by FortiWeb attack logs.

FortiView

Bug ID	Description
542607	When the user drills down in <i>Applications & Websites > Top Web Sites (FortiClient)</i> , the page shows "No entry found".
626530	<i>Bytes Sent/Received</i> should match the <i>Top Destinations</i> and <i>Policy Hit</i> charts under <i>FortiView</i> when filtered by the same policy ID.

Bug ID	Description
539298	Customer may not see data on cloud application bytes in FortiView.
579828	There may be a bandwidth discrepancy under <i>FortiView > Application & websites > Top websites</i> .
616675	Bandwidth may not match between FortiAnalyzer and FortiGate.
616914	Some graphs may not render data in FortiView.
620565	FortiAnalyzer should remove the entry <i>Reserved</i> in <i>Top Country/Region</i> .
638828	Incident of Compromised Hosts may not be triggered.
639523	FortiView DNS Logs may be empty.
640553	FortiView monitor WiFi widget is not showing Bridged SSID information.
641938	<i>Navigation to Monitors > Local System Performance</i> may cause the GUI to not respond.
642837	The GUI should indicate when Sandbox detection only supports FortiGate in Fabric ADOM.
643088	For VPN, the table keeps loading or returns <i>Server error: Invalid request-id ***** for fetching result</i> .
643842	All <i>SD-WAN Rule</i> related widgets or charts may show <i>No Data</i> in <i>Secure SD-WAN Monitor</i> and <i>Secure SD-Wan report</i> .
643843	<i>Monitors > Secure SD-WAN Monitor > SD-WAN Rules Utilization</i> widget always shows <i>No Data</i> .

FortiSoC

Bug ID	Description
632326	Syslog type <i>Event Handler Alert</i> sends an Email that is truncated.
638676	SNMP alert is not generated for event handler triggered by FortiWeb attack logs.

Log View

Bug ID	Description
579871	Restoration of logs does not indicate the correct timestamps under log browse after a NTP out of sync event.
608139	Opening compressed FortiClient traffic file on FortiAnalyzer may cause other compressed FortiClient traffic logs to fail to open.

Bug ID	Description
625306	Hiding column(s) in Log view may cause filters to reference the wrong column.
631527	FortiAnalyzer may show a negative value for sent or received packet count under <i>Log View > Traffic</i> .
591272	Downloaded Logs files from <i>Log View</i> or <i>Browse</i> are not in the correct CSV format.
604850	The remote IP for SSL-VPN is showing as <i>IPsec Remote IP</i> .
633393	Some of the IPS archive files do not contain whole <i>Attack Context</i> but only contain <i>BODY</i> that is partial part of <i>Attack Context</i> .
635598	FortiAnalyzer may not display Traffic Logs in <i>Log View</i> and return <i>Web Server Error 500</i> .
641013	After creating an ADOM for FortiMail, the ADOM is not visible on GUI and mail domain logs are not going to the default FortiMail ADOM.
643858	Actual analytic logs does not match what is observed in log view.
644189	Filters configured in the FortiView summary are not applied to <i>Log View</i> .
646775	<i>Log View > Fabric > All > Source IP</i> filter with unspecific conditions may show <i>No entry found</i> .
650857	<i>Source IP</i> in <i>Add Filter</i> box under <i>Log View</i> is not translated in Japanese.
651256	Username starting with a small case <i>vd</i> letter does not get displayed in the <i>Historical</i> logs.
652076	Searching takes a very long time when using <i>Custom Time Period</i> in <i>Log View</i> .

Others

Bug ID	Description
595696	The change of value for <code>system.global.enc-algorithm</code> is not applied to <code>oftpd</code> until a reboot.
617669	File parser may keep crashing every few minutes.
531962	There may be high disk I/O usage on FortiAnalyzer-1000E.
578907	<i>exec log-aggregate all</i> should aggregate all log files without any error.
587988	FortiAnalyzer is unable to send its local logs to FortiManager when FortiAnalyzer feature enabled.
616163	FortiAnalyzer may randomly display menu in Spanish instead of English.
625343	FortiAnalyzer may consume high on I/O resources every hour by fazwatch.
632971	FortiAnalyzer should have the ability to query CPU utilization on individual CPU core.
635984	Database rebuild may be slow.
644034	FortiAnalyzer HA may not synchronize analytics.

Bug ID	Description
651230	SQL database log insertion stops and stops rebuild if there are old archive logs.
652438	FortiAnalyzer may not perform a complete FTP backup because of problems with files.
651057	System may randomly generate PS failure messages on power(PS*) status changed to not-present.

Reports

Bug ID	Description
547496	FortiAnalyzer generates a report for selected device with outputs for all devices.
624911	FortiAnalyzer may not be able to generate the <i>SaaS Application Usage Report with Obfuscate User</i> feature.
522729	Report language files may not be fully translated.
621744	Reports may should incorrect columns and format when exporting from SSL Dialup IPSec to chart.
628823	FortiAnalyzer is not generating all local Event logs for reports.
645290	<i>Security Analysis</i> report is not showing <i>Traffic Bandwidth</i> chart.
647868	After upgrade, all default reports and event handler list are lost.
652715	The pre-defined reports items should be created in the new ADOM even when the same name being re-used.
653532	Scheduled report does not run if the report owner has been deleted from the admin list.

System Settings

Bug ID	Description
602422	Test User credentials fail when using RADIUS MSCHAPv2 as authentication type.
597443	FortiAnalyzer should able to forward logs that comply with syslog in RFC 5424 format.
628025	Power off without shutting down OS after clicking shutdown button on Hyper-V manager.
629663	Free text filter does not work when using (~) tilde sign on syslog ADOM for the message field.
630654	Imported logs may not sync to secondary device.
639102	FortiAnalyzer may not apply the <i>Not equal to</i> operator when <i>Log Forwarding > Log Filter</i> is configured using the GUI.

Bug ID	Description
645101	SAML GUI does not populate certificates into the combo-box after the certificates are inserted.
648105	The <i>License Information</i> widget displays <i>Unlimited</i> VM Storage when the correct license is <i>500 GB</i> .
653371	The CEF log forwarding start time does not match the event time.
647724	FortiAnalyzer may not be able to forward the same amount of logs in CEF format than in Syslog.

Appendix A - Recommended maximum number of ADOMs supported

FortiAnalyzer supports a recommended number of ADOMs based on the version.

Recommended maximum number of ADOMs supported for hardware versions:

FortiAnalyzer Platform	Maximum number of ADOMs
Desktop models	1
200F/300F/400F	25
800F/ 1000 Series	50
2000 Series	250
3000 Series	500
3700F and higher	800

Recommended maximum number of ADOMs supported for VMs:

FortiAnalyzer Platform	Maximum number of ADOMs
FAZ-VM-BASE (1 GB/Day)	5
1 GB/Day < License <= 5 GB/Day	10
5 GB/Day < License <= 25 GB/Day	25
25 GB/Day < License <= 100 GB/Day	50
100 GB/Day < License <= 500 GB/Day	250
500 GB/Day < License <= 1000 GB/Day	500
1000 GB/Day < License <= 5000 GB/Day	800
License > 5000 GB/Day	1100



FORTINET®



Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.