



FortiAnalyzer - Release Notes

Version 6.4.6

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/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



January 5, 2022

FortiAnalyzer 6.4.6 Release Notes

05-646-721292-20220105

TABLE OF CONTENTS

Change Log	5
FortiAnalyzer 6.4.6 Release	6
Supported models	6
FortiAnalyzer VM subscription license	6
FortiRecorder	7
Supported models for FortiRecorder	7
Supported cameras	7
Special Notices	8
FortiDeceptor logs	8
Hyperscale firewall mode	8
FortiAnalyzer 3700F performance issues	9
Citrix XenServer default limits and upgrade	9
FortiAnalyzer Cloud VM does not support FortiGate 6.4.0	9
FortiAnalyzer VM upgrade requires more memory	9
Maximum ADOM limits for FortiAnalyzer	10
Port 8443 reserved	10
All OFTP connections must be encrypted for FortiAnalyzer 6.2.0 (or higher)	10
Hyper-V FortiAnalyzer-VM running on an AMD CPU	10
SSLv3 on FortiAnalyzer-VM64-AWS	10
Upgrade Information	11
Downgrading to previous versions	11
Firmware image checksums	11
FortiAnalyzer VM firmware	11
SNMP MIB files	13
Product Integration and Support	14
FortiAnalyzer version 6.4.6 support	14
Web browsers	14
FortiOS/FortiOS Carrier	15
FortiADC	15
FortiAnalyzer	15
FortiAuthenticator	15
FortiCache	15
FortiClient	15
FortiDDoS	16
FortiDeceptor	16
FortiMail	16
FortiManager	16
FortiNAC	17
FortiProxy	17
FortiSandbox	17
FortiSwitch ATCA	17
FortiWeb	17
Virtualization	18

Feature support	18
Language support	19
Supported models	20
FortiGate models	21
FortiCarrier models	23
FortiADC models	24
FortiAnalyzer models	25
FortiAuthenticator models	26
FortiCache models	26
FortiDDoS models	26
FortiDeceptor models	27
FortiMail models	27
FortiNAC models	28
FortiProxy models	28
FortiSandbox models	28
FortiSwitch ATCA models	29
FortiWeb models	29
Resolved Issues	31
Device Manager	31
Event Management	31
FortiSOC	31
FortiView	32
Log View	32
Others	33
Reports	34
System Settings	34
Common Vulnerabilities and Exposures	34
Known Issues	36
Device Manager	36
FortiSOC	36
FortiView	36
Log View	37
Others	38
Reports	38
System Settings	38
Appendix A - Default and maximum number of ADOMs supported	39
Hardware models	39
Virtual Machines	40
FortiAnalyzer subscription license	40
FortiAnalyzer perpetual license	40

Change Log

Date	Change Description
2021-06-01	Initial release of 6.4.6.
2021-06-02	Moved 613115 from Known Issues to Resolved Issues on page 31 .
2021-06-08	Updated Known Issues on page 36 .
2021-06-10	Updated FortiGate models on page 21 and added 724625 to Known Issues on page 36 .
2021-06-14	Updated Resolved Issues on page 31 .
2021-06-24	Updated FortiGate models on page 21 and FortiCarrier models on page 23 .
2021-06-29	Updated Known Issues on page 36 .
2021-07-09	Added support for FortiSandbox 4.0 to FortiSandbox on page 17 and FortiSandbox models on page 28 .
2021-07-22	Updated FortiMail on page 16 . Updated FortiClient on page 15 .
2021-07-26	Moved 687809 from Resolved Issues to Known Issues on page 36 .
2021-08-9	Updated FortiGate models on page 21 .
2021-08-30	Updated FortiAuthenticator models on page 26 .
2021-09-01	Updated FortiWeb models on page 29 .
2021-09-14	Updated Appendix A - Default and maximum number of ADOMs supported on page 39 .
2021-09-15	Added <i>FortiDeceptor logs</i> to Special Notices on page 8 .
2021-09-17	Updated <i>FortiDeceptor logs</i> in Special Notices on page 8 . Removed 691220 from Known Issues on page 36 .
2021-11-09	Added FortiGate-2600F, FortiGate-2601F, FortiGate-2600F-DC, and FortiGate-2601F-DC to FortiGate models on page 21 .
2021-11-24	Updated FortiOS/FortiOS Carrier on page 15 , FortiGate models on page 21 , and FortiCarrier models on page 23 .
2022-01-05	Added FAZ-3700G to Supported models on page 6 .

FortiAnalyzer 6.4.6 Release

This document provides information about FortiAnalyzer version 6.4.6 build 2363.



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 6.4.6 supports the following models:

FortiAnalyzer	FAZ-150G, FAZ-300G, FAZ-200F, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-800G, FAZ-1000E, FAZ-2000E, FAZ-3000E, FAZ-1000F, FAZ-3000F, FAZ-3000G, FAZ-3500E, FAZ-3500F, FAZ-3500G, FAZ-3700F, FAZ-3700G, 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 11](#).

See also [Appendix A - Default and maximum number of ADOMs supported on page 39](#).



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 6.4.6.

FortiDeceptor logs

Logs sent from FortiDeceptor to FortiAnalyzer 6.4 may not display in FortiAnalyzer GUI because of an incorrect ADOM type for FortiDeceptor. You can reset the FortiDeceptor ADOM type in FortiAnalyzer to workaround this issue.



This issue is fixed in FortiAnalyzer 6.4.4 and later. However if the FortiDeceptor ADOM type is incorrect before upgrading to FortiAnalyzer 6.4.4 or later, you must still reset the FortiDeceptor ADOM type to correct the issue.

To reset the FortiDeceptor ADOM type:

1. In FortiAnalyzer, reset the FortiDeceptor ADOM by running the following command:
`execute reset adom-settings FortiDeceptor 3 1 18`
2. Ensure that the FortiDeceptor ADOM type is *FDC* by running the following command:
`diag dvm adom list`
3. From FortiDeceptor, sends logs again to FortiAnalyzer.
FortiDeceptor displays as an unregistered device in FortiAnalyzer.
4. In FortiAnalyzer, authorize the FortiDeceptor device.

Hyperscale firewall mode

FortiAnalyzer does not support logs from the following models when they have hyperscale firewall mode and netflow enabled:

- FortiGate-1800F
- FortiGate-1801F
- FortiGate-4200F
- FortiGate-4201F
- FortiGate-4400F
- FortiGate-4401F

FortiAnalyzer only supports logs when the normal firewall mode with standard FortiGate logging are enabled.

FortiAnalyzer 3700F performance issues

FortiAnalyzer 3700F models running version 6.0.3 and later may experience high *Disk I/O Utilization*, large differences between *Insert Rate Vs Receive Rate*, and large *Log Insert Lag Time*.

To prevent these performance issues, FortiAnalyzer allows the disk cache to warm up for 30 minutes before inserting logs into the SQL database.

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 - Default and maximum number of ADOMs supported on page 39](#).

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 6.4.6.



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 11](#)
- [Firmware image checksums on page 11](#)
- [FortiAnalyzer VM firmware on page 11](#)
- [SNMP MIB files on page 13](#)

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 the following virtualization environments: Aliyun, Amazon Web Services, Citrix and Open Source XenServer, Linux KVM, Microsoft Azure, Microsoft Hyper-V Server, and VMware ESX/ESXi.

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 Data Sheet](#) available on the Fortinet web site. 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 6.4.6 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 6.4.6 support on page 14](#)
- [Feature support on page 18](#)
- [Language support on page 19](#)
- [Supported models on page 20](#)

FortiAnalyzer version 6.4.6 support

This section identifies FortiAnalyzer version 6.4.6 product integration and support information:

- [Web browsers on page 14](#)
- [FortiOS/FortiOS Carrier on page 15](#)
- [FortiAnalyzer on page 15](#)
- [FortiAuthenticator on page 15](#)
- [FortiCache on page 15](#)
- [FortiClient on page 15](#)
- [FortiDDoS on page 16](#)
- [FortiMail on page 16](#)
- [FortiManager on page 16](#)
- [FortiProxy on page 17](#)
- [FortiSandbox on page 17](#)
- [FortiSwitch ATCA on page 17](#)
- [FortiWeb on page 17](#)
- [Virtualization on page 18](#)



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

Web browsers

This section lists FortiAnalyzer version 6.4.6 product integration and support for web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 88

- Google Chrome version 91

FortiOS/FortiOS Carrier

This section lists FortiAnalyzer version 6.4.6 product integration and support for FortiOS/FortiOS Carrier:

- 6.4.0 to 6.4.6
- 6.2.0 to 6.2.9
- 6.0.0 to 6.0.12

FortiADC

This section lists FortiAnalyzer version 6.4.6 product integration and support for FortiADC:

- 6.0.2
- 5.4.4

FortiAnalyzer

This section lists FortiAnalyzer version 6.4.6 product integration and support for FortiAnalyzer:

- 6.4.0 to 6.4.5
- 6.2.0 to 6.2.7
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiAuthenticator

This section lists FortiAnalyzer version 6.4.6 product integration and support for FortiAuthenticator:

- 6.0 to 6.2
- 5.0 to 5.5
- 4.3.0 and later

FortiCache

This section lists FortiAnalyzer version 6.4.6 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

FortiClient

This section lists FortiAnalyzer version 6.4.6 product integration and support for FortiClient:

- 6.4.0 and later
- 6.2.1 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

FortiDDoS

This section lists FortiAnalyzer version 6.4.6 product integration and support for FortiDDoS:

- 5.4.1
- 5.3.1
- 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

FortiDeceptor

This section lists FortiAnalyzer version 6.4.6 product integration and support for FortiDeceptor:

- 3.1.1

FortiMail

This section lists FortiAnalyzer version 6.4.6 product integration and support for FortiMail:

- 6.4.0 and later
- 6.2.0 and later
- 6.0.10 and later
- 5.4.12
- 5.3.13

FortiManager

This section lists FortiAnalyzer version 6.4.6 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

FortiNAC

This section lists FortiAnalyzer version 6.4.6 product integration and support for FortiNAC:

- 8.7.6
- 8.6.5
- 8.5.4

FortiProxy

This section lists FortiAnalyzer version 6.4.6 product integration and support for FortiProxy:

- 1.0 to 1.2

FortiSandbox

This section lists FortiAnalyzer version 6.4.6 product integration and support for FortiSandbox:

- 4.0.0
- 3.2.2
- 3.1.4
- 3.0.6
- 2.5.2
- 2.4.1
- 2.3.3
- 2.2.2

FortiSwitch ATCA

This section lists FortiAnalyzer version 6.4.6 product integration and support for FortiSwitch ATCA:

- 5.0.0 and later

FortiWeb

This section lists FortiAnalyzer version 6.4.6 product integration and support for FortiWeb:

- 6.3.0 to 6.3.10
- 6.2.0 to 6.2.4
- 6.1.0 to 6.1.2
- 6.0.0 to 6.0.7
- 5.9.0 to 5.9.1
- 5.8.0 to 5.8.6

- 5.7.0 to 5.7.1
- 5.6.0 to 5.6.1
- 5.5.0 to 5.5.6
- 5.4.1

Virtualization

This section lists FortiAnalyzer version 6.4.6 product integration and support for virtualization:

- Amazon Web Services (AWS)
- Citrix XenServer 6.0+ and Open Source Xen 4.1+
- Linux KVM
- Microsoft Azure
- Microsoft Hyper-V 2008 R2/2012/2012 R2/2016/2019
- VMware ESX/ESXi 5.5/6.0/6.5/6.7/7.0
- Nutanix AHV (AOS 5.10.5)
- Google Cloud (GCP)
- Oracle Cloud Infrastructure (OCI)
- Alibaba Cloud (AliCloud)

Feature support

The following table lists FortiAnalyzer feature support for log devices.

Platform	Log View	FortiView	Event Management	Reports
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiADC	✓		✓	
FortiAnalyzer	✓		✓	
FortiAuthenticator	✓			
FortiCache	✓		✓	✓
FortiClient registered to FortiGate	✓	✓		✓
FortiClient registered to FortiClient EMS	✓	✓		✓
FortiDDoS	✓	✓	✓	✓

Platform	Log View	FortiView	Event Management	Reports
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		✓
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 6.4.6. 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 21](#)
- [FortiCarrier models on page 23](#)
- [FortiADC models on page 24](#)
- [FortiAnalyzer models on page 25](#)
- [FortiAuthenticator models on page 26](#)
- [FortiCache models on page 26](#)
- [FortiDDoS models on page 26](#)
- [FortiDeceptor models on page 27](#)
- [FortiMail models on page 27](#)
- [FortiNAC models on page 28](#)
- [FortiProxy models on page 28](#)
- [FortiSandbox models on page 28](#)
- [FortiSwitch ATCA models on page 29](#)
- [FortiWeb models on page 29](#)

FortiGate models

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-41F, FortiGate-41F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, 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-200F, FortiGate-201F, 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-1800F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, 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 6000 Series: FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F, FortiGate-6300F-DC, FortiGate-6301F-DC, FortiGate-6500F-DC, FortiGate-6501F-DC FortiGate 7000 Series: FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7000F, FortiGate-7121F FortiGate DC: FortiGate-800D-DC, FortiGate-1500D-DC, FortiGate-2600F-DC, FortiGate-2601F-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-40F, FortiWiFi-40F-3G4G, FortiWiFi-41F, FortiWiFi-41F-3G4G, 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 FortiGateRugged: FortiGateRugged-60F, FortiGateRugged-60F-3G4G	6.4

Model	Firmware Version
FortiGate: FortiGate-30E, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-41F, FortiGate-41F-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-80F, FortiGate-80F-BypassFortiGate-81E, FortiGate-81E-POE, FortiGate-81F, 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-1800F, FortiGate-1801F, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 FortiGate 6000 Series: FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F, FortiGate-6300F-DC, FortiGate-6301F-DC, FortiGate-6500F-DC, FortiGate-6501F-DC FortiGate 7000 Series: FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7000F, FortiGate-7121F 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-40F, FortiWiFi-40F-3G4G, FortiWiFi-41F, FortiWiFi-41F-3G4G, 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, FortiGateRugged-60F, FortiGateRugged-60F-3G4G FortiOS: FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	6.2

Model	Firmware Version
FortiGate: FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-GBL, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-40F, FG-40F-3G4G, FG-41F, FG-41F-3G4G, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, 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-600E, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FortiGate-1800F, FortiGate-1801F, 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 6000 Series: FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F, FortiGate-6300F-DC, FortiGate-6301F-DC, FortiGate-6500F-DC, FortiGate-6501F-DC FortiGate 7000 Series: FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7000F, FortiGate-7121F 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-40F, FWF-40F-3G4G, FWF-41F, FWF-41F-3G4GFWF-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

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 6000 Series: FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC	6.4

Model	Firmware Version
FortiCarrier 7000 Series: FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7000F, FortiCarrier-7121F 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	
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 FortiCarrier 6000 Series: FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC FortiCarrier 7000 Series: FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7000F, FortiCarrier-7121F 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 FortiCarrier 6000 Series: FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6301F, FortiCarrier-6500F, FortiCarrier-6501F, FortiCarrier-6300F-DC, FortiCarrier-6301F-DC, FortiCarrier-6500F-DC, FortiCarrier-6501F-DC FortiCarrier 7000 Series: FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7000F, FortiCarrier-7121F 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

FortiADC models

Model	Firmware Version
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	6.0

Model	Firmware Version
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	5.4

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, 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	5.2

Model	Firmware Version
FortiAnalyzer VM: FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	
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	5.0
FortiAnalyzer VM: FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E	6.0 to 6.2
FortiAuthenticator VM: FAC-VM	
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000B, FAC-3000D, FAC-3000E	5.0 to 5.5
FortiAuthenticator VM: FAC-VM	
FortiAuthenticator: FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E	4.3
FortiAuthenticator VM: FAC-VM	

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	

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

Model	Firmware Version
FortiDDoS: FI-1500E, FI-2000E	5.0
FortiDDoS: FI-200B, FI400B, 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

FortiDeceptor models

Model	Firmware Version
FortiDeceptor: FDC-1000F, FDC-3000D	3.1
FortiDeceptor VM: FDC-VM	

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-60D, FML-200D, FML-1000D, FML-3000D, FML-200E, FML-400E, FML-2000E, FML-3000E, FML-3200E, FML-200F, FML-400F, FML-900F FortiMail VM: FE-VM64, FE-VM64-HV, FE-VM64-XEN	6.4
FortiMail: FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-60D, FML-200D, FML-1000D, FML-3000D, FML-200E, FML-400E, FML-2000E, FML-3000E, FML-3200E, FML-200F, FML-400F, FML-900F FortiMail VM: FE-VM64, FE-VM64-HV, FE-VM64-XEN	6.2
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

Model	Firmware Version
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

FortiNAC models

Model	Firmware Version
FortiNAC-500, FortiNAC-600, FortiNAC-700, FortiNAC-C-1000C, FortiNAC-C-2000C, FortiNAC-C-VM, FortiNAC-CA-VM, FortiNAC-M-VM, FortiNAC-Manager-550	8.7
FortiNAC-500, FortiNAC-600, FortiNAC-700, FortiNAC-C-1000C, FortiNAC-C-2000C, FortiNAC-C-VM, FortiNAC-CA-VM, FortiNAC-M-VM, FortiNAC-Manager-550	8.6
FortiNAC-500, FortiNAC-600, FortiNAC-700, FortiNAC-C-1000C, FortiNAC-C-2000C, FortiNAC-C-VM, FortiNAC-CA-VM, FortiNAC-M-VM, FortiNAC-Manager-550	8.5

FortiProxy models

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

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-1000F, FSA-2000E, FSA-3000E FortiSandbox-VM: FSA-AWS, FSA-VM	4.0
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox-VM: FSA-AWS, FSA-VM	3.2
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

Model	Firmware Version
FortiSandbox: FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D	2.4.1
FortiSandbox VM: FSA-VM	2.3.3
FortiSandbox: FSA-1000D, FSA-3000D, FSA-3500D	2.2.0
FortiSandbox VM: FSA-VM	2.1.3
FortiSandbox: FSA-1000D, FSA-3000D	2.0.3
FortiSandbox VM: FSA-VM	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	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-400C, FortiWeb-3000C, FortiWeb-4000C, FortiWeb-3000CFSX, FortiWeb-100D, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-3000D, FortiWeb-4000D, FortiWeb-3000DFSX, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000E	6.3
FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	
FortiWeb: FortiWeb-400C, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-100D, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E	6.2
FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	

Model	Firmware Version
FortiWeb: FortiWeb-400C, FortiWeb-3000C, FortiWeb-4000C, FortiWeb-3000CFSX, FortiWeb-100D, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-3000D, FortiWeb-4000D, FortiWeb-3000DFSX, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000E FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XenServer	6.1
FortiWeb: FWB-400C, FWB-100D, 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
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
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
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-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7
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
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
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-XENSERVEN, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5
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-XENSERVEN, FWB-HYPERV	5.4

Resolved Issues

The following issues have been fixed in FortiAnalyzer version 6.4.6. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Device Manager

Bug ID	Description
521774	Add and delete function for unregistered devices are greyed out even when the root ADOM is locked.
523721	FortiAnalyzer should support FortiADC device type.
613115	<i>Device Manager</i> view may show red icons for VDOMs even when the log is received.
622649	When a FortiGate HA device is deleted, their log files are not deleted.
676662	Collector may not be showing the same FortiGate device version as analyzer.
681419	Notification icon may still be present for hidden unauthorized devices.

Event Management

Bug ID	Description
504426	Event list shall auto refresh after events are acknowledged and <i>Show Acknowledged</i> is disabled.

FortiSOC

Bug ID	Description
685426	FortiAnalyzer should be able to see the incident that corresponds to events under the incidents analysis page.

FortiView

Bug ID	Description
633960	Filter is empty in request when drill-down <i>Top Applications(FortiClient)</i> view to <i>Log View</i> .
682485	Policy hit count may be shown as zero while there is traffic.
682657	FortiView may not refresh correctly after switching between ADOMs.
683580	The <i>Not</i> operation may not work for advanced filter.
684131	<i>Top Sources</i> response may be slow when filter by policy ID.
684193	<i>Secure SD-WAN Monitor</i> should not send request when device list fails to load.
685452	The <i>NOT</i> filter filter may not work properly.
688141	FortiAnalyzer should be able to apply multiple negative filters from the same type.
690895	<i>FortiView > Monitors > Secure SD-WAN Monitor > SD-WAN Rules Utilization</i> widget may show <i>No Data</i> for some FortiGates.
692464	While retrieving IPS error log details, FortiAnalyzer may prompt XSS error.
692852	After upgrade, the <i>Secure SD-WAN Monitor</i> may have issues and show <i>No Data</i> for <i>Performance</i> , <i>Jitter</i> , <i>Latency</i> , or <i>Packet loss</i> widget.
702268	When accessing from FortiGate, loading the <i>FortiView</i> page may be very slow when the source is set as <i>FortiAnalyzer</i> .
708006	<i>Monitors Endpoints</i> does not show all FortiClient endpoints as in logs.
711810	<i>SSL Dialup IPsec connection</i> count may not match the connection list.
713083	FortiAnalyzer may show a <i>No Data</i> message for the <i>Worldwide Threat Prevalence</i> chart.

Log View

Bug ID	Description
600083	<i>Endpoint Identification</i> should always show the same user tied to the same session.
604850	The remote IP for SSL-VPN is showing as <i>IPsec Remote IP</i> .
652076	Log view may take a while to load with <i>Custom Time Period</i> .
660792	FortiAnalyzer-1000E may take a long time to download a filtered log view file.
686258	FortiAnalyzer may return <i>No entry found</i> when the Log View filter has many devices selected.
686924	Downloading CSV file contains <code>tunnel-up</code> and <code>tunnel-down</code> VPN logs from other devices that belong to different ADOMs.

Bug ID	Description
690922	The event logs filter should display logs only from its own VDOM.
694307	When increasing in memory usage, FortiAnalyzer may stop receiving logs via OFTP from FortiGate devices.
704410	FortiAnalyzer may stop handling logs and the <code>oftpd</code> process becomes non-responsive.
711711	Log filter may show unfiltered values.

Others

Bug ID	Description
656370	FortiAnalyzer SCP backup cannot be stopped.
671711	SQL database rebuild may not start and return <i>ERROR: sqlplugind(690):receiver.c:96: socket 70 poll() failed.</i>
677494	FortiAnalyzer may return SQL query error when creating temporary table <code>blk1st</code> during <code>ioc-rescan</code> . Workaround: Please set <code>ioc-rescan</code> days to less than database compression days.
679268	FortiAnalyzer is not able to backup via SFTP on a custom port.
681884	HA synchronization may stall at random percentage.
682997	FortiAnalyzer may show <code>fmgd</code> crash during boot up after upgrade.
686491	<code>Postgres</code> may keep causing OoM with segmentation faults on multiple processes.
690271	The <code>sqllogd</code> daemon may crash.
693161	When frequently accessing different pages, FortiAnalyzer's GUI may become sluggish and pages may not transition.
696211	Secondary FortiAnalyzer accepts FTP connections after disabling FortiRecorder.
697654	FortiAnalyzer may return duplicated data within log view JSON response.
698780	FortiAnalyzer may intermittently provide empty response to FortiView JSON requests.
700562	When creating a system admin user using JSON API, FortiAnalyzer may return an error: <i>The data is invalid for selected url.</i>
702140	The <code>disable-module</code> setting resets to default after reboot.
709699	FortiAnalyzer may contain a few <code>siemdb</code> crashes.
710178	FortiAnalyzer is listening on TCP/3000 even though <code>accept-aggregation</code> is disabled.
713826	The <code>diagnose test application siemdbd 6</code> command may show wrong information after removing the last ADOM with <i><code>diagnose siem remove database</code></i> .

Reports

Bug ID	Description
683668	FortiClient report is always empty after enabled device filter.
692097	Report's sub-charts may not work after upgrade.
704544	Application icons may not be displayed in report.
710409	<i>Top5-Users-By-Bandwidth</i> drill-down chart result may contain SQL error.
713189	<i>Dataset</i> and <i>Intrusions-Timeline-By-Severity</i> , may not list low severity intrusions.
718579	While creating new or editing an Output Profile, the body section does not take any input.
720897	Scheduled Report may not run when the <code>/tmp</code> folder is full.

System Settings

Bug ID	Description
560895	FortiAnalyzer should separate the Admin profile setting for Log and SoC views.
613526	FortiAnalyzer VM should prompt a warning when reaching the maximum ADOM limit.
626636	The <i>Allow</i> button may now work in HA configuration page.
631709	Email should successfully sent out from FortiAnalyzer with <i>SMTPS TCP/465</i> .
634253	ADOMs may disappear randomly from ADOM configuration while editing it.
668901	After enabling <i>Collector</i> mode, FortiAnalyzer may not show FortiView.
681321	Avatar may keep synchronizing which results in <i>init sync cannot be finished</i> .
685892	FortiAnalyzer is not sending <i>SMTP EHLO</i> message with fully-qualified hostname.
689824	After upgrade, log filter setting may set to <i>Equal to</i> for log forwarding.
691798	The secondary unit in FortiAnalyzer HA cluster may report <i>HA cluster config-sync DOWN, cause=keepalive failure</i> every couple of days.
696041	FortiAnalyzer SSO should support URI format in entity ID.
708047	They may be multiple <code>devid</code> , <code>devname</code> , or <code>tz</code> columns when log is forwarded in syslog.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
672953	FortiAnalyzer 6.4.6 is no longer vulnerable to the following CVE-Reference: <ul style="list-style-type: none">• CVE-2021-24022

Known Issues

The following issues have been identified in FortiAnalyzer version 6.4.6. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Device Manager

Bug ID	Description
639479	FortiGate v6.0 with <i>sub-ca</i> certificate may not be able to establish oftp connection with FortiAnalyzer without sub-ca certificate.
696853	When manually adding a device in FortiNAC ADOM, version v8.8 is not listed in the version option.
716486	FortiAnalyzer still populating unauthorized device list even after <i>detect-unregistered-log-device</i> is set to <i>disable</i> .

FortiSOC

Bug ID	Description
668942	A playbook running AV scan on endpoint may return error: <i>failed results- can not find parameters for connector</i> .

FortiView

Bug ID	Description
539298	Customer may not see data on cloud application bytes in FortiView.
579828	There may be bandwidth discrepancy under <i>FortiView > Application & websites > Top websites</i> .
616675	Bandwidth may not match between FortiAnalyzer and FortiGate.
626530	Bytes Sent/Received should match between <i>Top Destinations</i> and <i>Policy Hit</i> charts under FortiView when filtered by the same policy ID.
640553	FortiView monitor WiFi widget is not showing <i>Bridged SSID</i> information.

Bug ID	Description
641596	FortiAnalyzer may show <i>No Data</i> in <i>User Vulnerabilities Summary</i> widget.
642837	The GUI should indicate if Sandbox detection only supports FortiGate in Fabric ADOM.
663930	Ports status may not be incorrect in <i>Secure SD-WAN Monitor</i> and <i>SD-WAN Performance</i> status.
667076	<i>FortiView Top Cloud Users</i> may show <i>no entry found</i> message but there is a session graph shown.
683525	The return lines may be incorrect after adding filters to <i>Top Website Categories</i> .
688537	Information <i>End User</i> located in <i>Summary</i> should match with time range and logs.
707480	<i>Top Threats(FortiClient)</i> may only display Threat level <i>LOW</i> and <i>Allowed</i> incidents.
721008	<i>Threats > Compromised Hosts</i> may not be able to acknowledge compromised hosts when the end user is not a known IP.
691570	FortiAnalyzer may not be able to cancel <i>IOC re-scan</i> task.

Log View

Bug ID	Description
608139	Opening compressed FortiClient traffic file on FortiAnalyzer may cause other compressed FortiClient traffic logs fail to open.
633393	Some IPS archive files only contain <i>BODY</i> of <i>Attack Context</i> instead of the whole <i>Attack Context</i> .
635598	FortiAnalyzer may not display Traffic Logs in Log View and return Web Server Error 500.
641013	After created ADOM for FortiMail, the ADOM is not visible on GUI and mail domain logs are not going to the default FortiMail ADOM.
653765	Some log files under Log Browse may contain a mix of event and traffic messages.
661094	In Log View, importing log may fail.
674027	Filtering FortiClient event logs with wildcard <i>UID</i> filter returns no data.
704206	When filtering with <i>Action</i> and <i>Source IP</i> under the <i>Traffic</i> menu, the filter output may be incorrect with the combination of smart action with any other field.

Others

Bug ID	Description
584105	The <code>/drive0/private/restapi/sync/fgt_intf_stat</code> location may use too much inodes.
616355	FortiGate may display <i>SSL error</i> or <i>OFTP error</i> when testing connectivity with FortiAnalyzer.
632971	FortiAnalyzer should have the ability to query CPU utilization on individual CPU core.
660810	FortiAnalyzer-200F rebuild may get stuck and <i>sqllogd</i> may crash due to insufficient memory.
687809	Log insert lag time may go above 5 hours on a properly sized FortiAnalyzer.
701753	SIEM database should be trimmed at the same time when quota enforcement occurs.
724625	Upgrade from 6.4.6 to 7.0.0 will result in all configuration being lost.

Reports

Bug ID	Description
628823	FortiAnalyzer is not generating all local Event logs for reports.
653207	FortiAnalyzer may have incorrect dataset queries without considering the <i>direction</i> field.
677090	<i>Report Filter</i> may not work with <i>devname</i> .

System Settings

Bug ID	Description
629663	Free text filter does not work when using (~) tilde sign on syslog ADOM for the <code>msg</code> field.
630654	Imported logs may not sync to slave.
638380	FortiAnalyzer may accept invalid which may break some widgets.
653371	CEF log forwarding start time does not match with event time.
669402	FortiAnalyzer may not time out admin a session after many hours.
717524	Users may not be able to add a username which contains a Slash "/" inside <i>Device Log Setting</i> .

Appendix A - Default and maximum number of ADOMs supported

This section identifies the supported number of ADOMs for FortiAnalyzer hardware models and virtual machines.

See also the [FortiAnalyzer Data Sheet](#).

Hardware models

FortiAnalyzer supports a default number of ADOMs based on hardware model.

Some hardware models support an ADOM subscription license. When you purchase an ADOM subscription license, you increase the number of supported ADOMs. For example, you can purchase an ADOM subscription license for the FAZ-3000G series, which allows you to use up to a maximum of 1200 ADOMs.

Other hardware models do not support the ADOM subscription license. For hardware models that do not support the ADOM subscription license, the default and maximum number of ADOMs is the same.

FortiAnalyzer Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
Desktop models	1	-	1
150G Series	3	-	3
200F/300F/400E	25	-	25
300G Series	25	-	25
800F/1000F Series	50	-	50
2000E Series	250	-	250
3000F Series	500	-	500
3000G Series	500	✓	1200
3500G Series	500	-	500
3700F Series and higher	1200	-	1200

Virtual Machines

FortiAnalyzer subscription license

Five (5) ADOMs are included with FortiAnalyzer VM subscription licenses. Licenses are non-stackable. Additional ADOMs can be purchased with an ADOM subscription license.

FortiAnalyzer perpetual license

Recommended maximum number of ADOMs supported:

FortiAnalyzer Platform	Default 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	1200



FORTINET®



Copyright© 2022 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.