



# FortiAnalyzer - Release Notes

Version 6.2.5

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

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

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

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



July 31, 2020

FortiAnalyzer 6.2.5 Release Notes

05-625-634824-20200731

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>FortiAnalyzer 6.2.5 Release</b>	<b>6</b>
Supported models	6
<b>Special Notices</b>	<b>7</b>
Logger field not added to incoming FortiGate logs resulting in empty charts	7
Newly deployed, factory reset, or disk format may trigger upgrade code on subsequent reboot	7
Maximum ADOM limits for FortiAnalyzer	7
Port 8443 reserved	8
All OFTP connections must be encrypted for FortiAnalyzer 6.2.0 (or higher)	8
Hyper-V FortiAnalyzer-VM running on an AMD CPU	8
SSLv3 on FortiAnalyzer-VM64-AWS	8
Pre-processing logic of ebtime	8
<b>Upgrade Information</b>	<b>9</b>
Downgrading to previous versions	9
Firmware image checksums	9
FortiAnalyzer VM firmware	10
SNMP MIB files	11
<b>Product Integration and Support</b>	<b>12</b>
FortiAnalyzer version 6.2.5 support	12
Web browsers	12
FortiOS/FortiOS Carrier	13
FortiAnalyzer	13
FortiAuthenticator	13
FortiCache	13
FortiClient	13
FortiDDoS	14
FortiMail	14
FortiManager	14
FortiProxy	14
FortiSandbox	14
FortiSwitch ATCA	15
FortiWeb	15
Virtualization	15
Feature support	15
Language support	16
Supported models	17
FortiGate models	18
FortiCarrier models	21
FortiDDoS models	22
FortiAnalyzer models	22
FortiMail models	23
FortiSandbox models	24

---

FortiSwitch ATCA models .....	24
FortiWeb models .....	24
FortiCache models .....	26
FortiProxy models .....	26
FortiAuthenticator models .....	26
<b>Resolved Issues .....</b>	<b>27</b>
Device Manager .....	27
FortiView .....	27
Log View .....	27
Others .....	28
Reports .....	28
System Settings .....	29
Common Vulnerabilities and Exposures .....	29
<b>Known Issues .....</b>	<b>30</b>
Device Manager .....	30
FortiView .....	30
Log View .....	30
Others .....	31
Reports .....	31
System Settings .....	32
<b>Appendix A - Recommended maximum number of ADOMs supported .....</b>	<b>33</b>

# Change Log

Date	Change Description
2020-05-15	Initial release of 6.2.5.
2020-05-19	Added bug 635070 to <a href="#">Known Issues on page 30</a> .
2020-05-25	Clarified recommended maximum number of ADOMs is not enforced by updating <a href="#">Special Notices on page 7</a> and <a href="#">Appendix A - Recommended maximum number of ADOMs supported on page 33</a> .
2020-05-26	Added FortiGate-40F/41F and FortiWiFi-40F/41F to <a href="#">FortiGate models on page 18</a> .
2020-06-17	Added bug 610898 to <a href="#">Resolved Issues on page 27</a> .
2020-06-18	Added bug 640634 to <a href="#">Known Issues on page 30</a> .
2020-06-26	Added bugs 597311 and 606144 to <a href="#">Resolved Issues on page 27</a> .
2020-06-29	Added FortiOS 6.0.10 to <a href="#">FortiOS/FortiOS Carrier on page 13</a> .
2020-07-31	Added special notice for 640634 to <a href="#">Special Notices on page 7</a> . Added bug 643238 to <a href="#">Known Issues on page 30</a> .

# FortiAnalyzer 6.2.5 Release

This document provides information about FortiAnalyzer version 6.2.5 build 1307.



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

---

This section includes the following topics:

- [Supported models on page 6](#)

## Supported models

FortiAnalyzer version 6.2.5 supports the following models:

<b>FortiAnalyzer</b>	FAZ-200F, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000E, FAZ-1000F, FAZ-2000E, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500G, FAZ-3500F, FAZ-3700F and FAZ-3900E.
<b>FortiAnalyzer VM</b>	FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer version 6.2.5.

## Logver field not added to incoming FortiGate logs resulting in empty charts

FortiAnalyzer adds a `logver` field to logs received from FortiGates. In FortiAnalyzer 6.2.5, FortiAnalyzer may stop adding the `logver` field in some cases. (See 640634 in [Known Issues on page 30](#).) If that happens, all charts that rely on the field are empty when reports are generated.

Upgrading to FortiAnalyzer 6.4.0 or later will resolve this issue.

Other options include:

1. As a workaround, modify the underlying datasets so that the `logver` field is not referenced. See technote [Missing field 'Logver' in logs causing reports to come out blank](#).
2. Contact technical support to obtain a FortiAnalyzer 6.2 special branch build that includes the fix. The fix for 6.2 is scheduled to be available in an upcoming release.

## Newly deployed, factory reset, or disk format may trigger upgrade code on subsequent reboot

For a newly deployed VM instance or appliance, a disk format or a factory reset on a FortiAnalyzer unit running version 6.2.3 may trigger the upgrade code upon rebooting the system, which in turn may update the database configuration, although no upgrades are required. This issue does not affect FortiAnalyzer units upgraded from versions prior to 6.2.3.

**Workaround:** Immediately after deploying a new FortiAnalyzer with version 6.2.3, reboot the system before administering any configuration.

## Maximum ADOM limits for FortiAnalyzer

FortiAnalyzer hardware devices and VMs display a warning when the recommended 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 33](#).

## 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
```

## Pre-processing logic of ebtime

Logs with the following conditions met are considered usable for the calculation of estimated browsing time:

Traffic logs with `logid` of 13 or 2, when `logid == 13`, `hostname` must not be empty. The `service` field should be either HTTP, 80/TCP or 443/TCP.

If all above conditions are met, then `devid`, `vdom`, and `user` (`srcip` if `user` is empty) are combined as a key to identify a user. For time estimation, the current value of `duration` is calculated against history session start and end time, only un-overlapped part are used as the `ebtime` of the current log.



# Upgrade Information

You can upgrade FortiAnalyzer 6.0.3 or later directly to 6.2.5.



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



Upgrading to FortiAnalyzer 6.0.2 from 6.0.0 or 6.0.1 is supported and does not trigger a log database rebuild.

---

This section contains the following topics:

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

## Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```

## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. To verify the integrity of the download, select the *Checksum* link next to the *HTTPS* download link. A dialog box will be displayed with the image file name and checksum code. Compare this checksum with the checksum of the firmware image.

## FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

### Aliyun

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains QCOW2 that can be used by qemu.

### Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

### Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the Citrix XenServer Disk (VHD), and OVF files.

### 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 6.2.5 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 6.2.5 support on page 12](#)
- [Feature support on page 15](#)
- [Language support on page 16](#)
- [Supported models on page 17](#)

## FortiAnalyzer version 6.2.5 support

This section identifies FortiAnalyzer version 6.2.5 product integration and support information:

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



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

---

### Web browsers

This section lists FortiAnalyzer version 6.2.5 product integration and support for web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 74

- Google Chrome version 80

## FortiOS/FortiOS Carrier

This section lists FortiAnalyzer version 6.2.5 product integration and support for FortiOS/FortiOS Carrier:

- 6.2.0 to 6.2.4
- 6.0.0 to 6.0.10
- 5.6.0 to 5.6.12
- 5.4.0 to 5.4.12

## FortiAnalyzer

This section lists FortiAnalyzer version 6.2.5 product integration and support for FortiAnalyzer:

- 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 6.2.5 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 6.2.5 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

## FortiClient

This section lists FortiAnalyzer version 6.2.5 product integration and support for FortiClient:

- 6.2.1
- 6.0.8
- 5.6.6
- 5.4.0 and later

## FortiDDoS

This section lists FortiAnalyzer version 6.2.5 product integration and support for FortiDDoS:

- 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 6.2.5 product integration and support for FortiMail:

- 6.2.1
- 6.0.6
- 5.4.10
- 5.3.13

## FortiManager

This section lists FortiAnalyzer version 6.2.5 product integration and support for FortiManager:

- 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 6.2.5 product integration and support for FortiProxy:

- 1.0

## FortiSandbox

This section lists FortiAnalyzer version 6.2.5 product integration and support for FortiSandbox:

- 3.1.0
- 3.0.5
- 2.5.2
- 2.4.1

- 2.3.3
- 2.2.2

## FortiSwitch ATCA

This section lists FortiAnalyzer version 6.2.5 product integration and support for FortiSwitch ATCA:

- 5.0.0 and later

## FortiWeb

This section lists FortiAnalyzer version 6.2.5 product integration and support for FortiWeb:

- 6.2.2
- 6.1.1
- 6.0.5
- 5.9.1
- 5.8.6
- 5.7.2
- 5.6.1
- 5.5.6
- 5.4.1

## Virtualization

This section lists FortiAnalyzer version 6.2.5 product integration and support for virtualization:

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

## Feature support

The following table lists FortiAnalyzer feature support for log devices.

Platform	Log View	FortiView	Event Management	Reports
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓

Platform	Log View	FortiView	Event Management	Reports
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		✓
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 6.2.5. Please ensure that the log devices are supported before completing the upgrade.



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

---

This section contains the following topics:

- [FortiGate models on page 18](#)
- [FortiCarrier models on page 21](#)
- [FortiDDoS models on page 22](#)
- [FortiAnalyzer models on page 22](#)
- [FortiMail models on page 23](#)
- [FortiSandbox models on page 24](#)
- [FortiSwitch ATCA models on page 24](#)
- [FortiWeb models on page 24](#)
- [FortiCache models on page 26](#)
- [FortiProxy models on page 26](#)
- [FortiAuthenticator models on page 26](#)

## FortiGate models

Model	Firmware Version
<p><b>FortiGate:</b> FortiGate-30E, FortiGate-30E-3G4G-GBL, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FortiGate-60F, FortiGate-61F, FortiGate-60E-POE, FortiGate-61E, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100F, FortiGate-101F, FortiGate-100F, FortiGate-101E, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FG-400E, FG-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-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E, FortiGate-3400E, FortiGate-3401E, FortiGate-3400E-DC, FortiGate-3401E-DC</p> <p><b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1</p> <p><b>FortiGate 6000 Series:</b> FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F</p> <p><b>FortiGate 7000 Series:</b> FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC</p> <p><b>FortiGate DC:</b> 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</p> <p><b>FortiGate Hardware Low Encryption:</b> FortiGate-80C-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC</p> <p><b>FortiWiFi:</b> 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</p> <p><b>FortiGate-VM:</b> 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</p> <p><b>FortiGate Rugged:</b> FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D</p> <p><b>FortiOS:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen</p>	6.2

Model	Firmware Version
<p><b>FortiGate:</b> 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-60F, FG-60D-POE, FG-60E, FG-60E-POE, FG-60F, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100F, FG-100F, FG-101F, 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, FG300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3400E, FG-3401E, FG-3600C, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-2200E, FG-2201E, FG-3300E, FG-3301E, FG-1100E, FG-1101E, FG-3400E, FG-3401E, FG-3400E-DC, FG-3401E-DC</p> <p><b>FortiGate 5000 Series:</b> FG-5001D, FG-5001E, FG-5001E1</p> <p><b>FortiGate 6000 Series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p><b>FortiGate 7000 Series:</b> FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC</p> <p><b>FortiGate DC:</b> FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC</p> <p><b>FortiGate Hardware Low Encryption:</b> FG-100D-LENC, FG-600C-LENC</p> <p><b>Note:</b> All license-based LENC is supported based on the FortiGate support list.</p> <p><b>FortiWiFi:</b> FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-40F, FWF-40F-3G4G, FWF-41F, FWF-41F-3G4G, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FW-60E-DSL, FW-60E-DSLJ, FWF-60F, FWF-61F, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D</p> <p><b>FortiGate VM:</b> 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</p> <p><b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D</p>	6.0
<p><b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-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><b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D, FG-5001E, FG-5001E1</p> <p><b>FortiGate 6000 Series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p><b>FortiGate 7000 Series:</b> FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC</p>	5.6

Model	Firmware Version
<p><b>FortiGate DC:</b> FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC, FG-7060E-8-DC</p> <p><b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC</p> <p><b>Note:</b> All license-based LENC is supported based on the FortiGate support list.</p> <p><b>FortiWiFi:</b> FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FW-60E-DSL, FW-60E-DSLJ, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D</p> <p><b>FortiGate VM:</b> FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-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><b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D</p>	
<p><b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100F, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-200E, FG-201E, FGT-300D, FGT-300E, FGT-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG 3800D, FG-3810D, FG-3815D, FG-3960E, FG3980E, FG-2000E, FG-2500E</p> <p><b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D, FG-5001E, FG-5001E1</p> <p><b>FortiGate 6000 Series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p><b>FortiGate 7000 Series:</b> FG-7030E-Q, FG-7030E-S, FG-7040E-1, FG-7040E-2, FG-7040E-3, FG-7040E-4, FG-7040E-5, FG-7040E-6, FG-7040E-8, FG-7040E-8-DC, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6, FG-7060E-8</p> <p>(Update only) FortiGate 7000 series: FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC</p> <p><b>FortiGate DC:</b> FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815DC, FG-7060E-8-DC</p> <p><b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC</p> <p><b>Note:</b> All license-based LENC is supported based on the FortiGate support list.</p> <p><b>FortiWiFi:</b> FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E-DSL, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D</p> <p><b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM</p>	5.4

Model	Firmware Version
<b>FortiGate Rugged:</b> FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D	

## FortiCarrier models

Model	Firmware Version
<p><b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1</p> <p><b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC</p> <p><b>FortiCarrier-VM:</b> 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</p>	6.2
<p><b>FortiCarrier:</b> FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E  <b>FortiCarrier-DC:</b> FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC</p> <p><b>FortiGate 6000 series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p><b>FortiGate 7000 series:</b> FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC</p> <p><b>FortiCarrier-VM:</b> 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</p>	6.0
<p><b>FortiCarrier:</b> 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</p> <p><b>FortiCarrier 6000 Series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p><b>FortiCarrier 7000 Series:</b> FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC</p> <p><b>FortiCarrier-DC:</b> 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</p> <p><b>FortiCarrier-VM:</b> 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</p>	5.6
<p><b>FortiCarrier:</b> 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</p> <p><b>FortiCarrier 6000 Series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F</p> <p><b>FortiCarrier 7000 Series:</b> FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC</p> <p><b>FortiCarrier-DC:</b> 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-7060E-8-DC</p>	5.4

Model	Firmware Version
<b>FortiCarrier-VM:</b> 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	

## FortiDDoS models

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

## FortiAnalyzer models

Model	Firmware Version
<b>FortiAnalyzer:</b> 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.	6.2
<b>FortiAnalyzer VM:</b> 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).	
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-200F, FAZ-300D, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000D, FAZ-1000E, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F and FAZ-3900E.	6.0
<b>FortiAnalyzer VM:</b> 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).	
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E.	5.6
<b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B.	5.4
<b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	

Model	Firmware Version
<b>FortiAnalyzer:</b> FAZ-100C, FAZ-200D, FAZ-200E, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B <b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
<b>FortiAnalyzer:</b> FAZ-100C, FAZ-200D, FAZ-200E, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B <b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

## FortiMail models

Model	Firmware Version
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-200F, FML-400F, FML-900F	6.2
<b>FortiMail:</b> 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
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E <b>FortiMail Low Encryption:</b> FE-3000C-LENC	5.4
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B <b>FortiMail Low Encryption:</b> FE-3000C-LENC <b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B <b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2
<b>FortiMail:</b> FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B <b>FortiMail VM:</b> FE-VM64	5.1
<b>FortiMail:</b> FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B <b>FortiMail VM:</b> FE-VM64	5.0

## FortiSandbox models

Model	Firmware Version
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox-VM:</b> FSA-AWS, FSA-VM	3.1
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-AWS, FSA-VM	3.0
<b>FortiSandbox VM:</b> FSA-KVM, FSA-VM	2.5.2
<b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-VM	2.4.1 2.4.0 2.3.3 2.3.2
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D, FSA-3500D <b>FortiSandbox VM:</b> FSA-VM	2.2.2 2.1.3
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D <b>FortiSandbox VM:</b> FSA-VM	2.0.3 1.4.2
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D	1.4.1 1.3.0 1.2.0 and later

## FortiSwitch ATCA models

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

## FortiWeb models

Model	Firmware Version
<b>FortiWeb:</b> 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



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

Model	Firmware Version
<b>FortiWeb:</b> FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E  <b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, and FWB-HYPERV	5.3.9
<b>FortiWeb:</b> FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E  <b>FortiWeb VM:</b> FWB-VM64, FWB-HYPERV, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR	5.2.4

## FortiCache models

Model	Firmware Version
<b>FortiCache:</b> FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E  <b>FortiCache VM:</b> FCH-VM64, FCH-KVM	4.0, 4.1, 4.2

## FortiProxy models

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

## FortiAuthenticator models

Model	Firmware Version
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E  <b>FortiAuthenticator VM:</b> FAC-VM, FAC-VM-HV, FAC-VM-KVM, FAC-VM-XEN	4.3, 5.0-5.5, 6.0

# Resolved Issues

The following issues have been fixed in FortiAnalyzer version 6.2.5. For inquiries about a particular bug, please contact [Customer Service & Support](#).

## Device Manager

Bug ID	Description
296528	Sorting with Device Manager's <i>Log Status</i> column may not work properly.
496394	Users may not be able to delete a VDOM from GUI or API.
589646	FortiAnalyzer should be able to add FortiProxy device with firmware version 1.2.
596832	FortiGate Cluster is removed from log forwarding on failover when FortiAnalyzer is managed by a FortiManager.

## FortiView

Bug ID	Description
562834	On <i>FortiView &gt; Top Sources</i> , FortiAnalyzer displays incorrect data when trying to filter logs with <i>Source</i> and <i>User</i> .
593374	Exported PDF should take into consideration how data is sorted.
595657	Drill-down Panel for Resource Usage in <i>SOC &gt; FortiView</i> may get stuck at loading.
602387	FortiAnalyzer may use high CPU resources when viewing logs from FortiGate.

## Log View

Bug ID	Description
542933	FortiView does not search logs for the time entered in custom time.
550523	Downloading logs from Log View randomly fails.
596232	JSON API 3.0 logfiles/data returns <code>adom privilege limit</code> error if the device is secondary.
608652	Event alert logs cannot be inserted into database successfully on HA primary unit.

## Others

Bug ID	Description
628352	FortiAnalyzer log-integrity check may fail.
508597	FortiAnalyzer with no devices may occupy high CPU resources by <code>sqllogd</code> .
529711	FortiAnalyzer may connect to map server and GeoIP server directly even when <code>web-proxy</code> is enabled.
551198	The command, <code>execute restore reports-config</code> , may not run correctly.
562540	FortiAnalyzer's diagnostic report should also include IO statistics.
568326	<code>oftpd</code> may keep crashing for several times a day.
569707	Device may hang and lose accessibility, including console.
590630	Backing up all ADOM logs via FTP may stop with no error printed.
591594	<code>snmpd</code> may frequently crash.
592593	FortiAnalyzer may update ADOM disk allocation or create ADOM without any checks when request is made via JSON API.
596192	FortiAnalyzer may return incorrect value for SNMP MIB <code>sysObjectID</code> .
596252	The <code>clusterd</code> daemon may consume high CPU resource.
597093	MIB file for FortiAnalyzer should not contain duplicated object ID.
601093	After upgrade, FortiManager may not receive logs from one FortiGate cluster that is running FortiOS 6.0.
617456	Disk space may be different between <code>execute lvm info</code> and other commands.

## Reports

Bug ID	Description
557388	There are discrepancies in <i>Bandwidth</i> and <i>Applications Report</i> for predefined datasets on the same report time period.
588590	FortiAnalyzer should print detailed message when importing report fails.
599987	Reports may not synchronize across HA pair.
608819	Report's hcache cannot be used on scheduled report when running on specific device.

## System Settings

Bug ID	Description
533885	Unnecessary message is popped up when deleting a fabric ADOM.
594693	FortiAnalyzer may show many messages on Alert Console: <i>re-obtained table size for FGTADOM1391-Elog-1553532000 size=8192.</i>
600639	FortiAnalyzer may not be able to move a VDOM with long name from the Root ADOM to another ADOM.
603346	FortiAnalyzer should not allow user to set to 0 day for data retention policy.
612328	When there are overlapping trust hosts, the incorrect IP and subnet might be used in the IP table.

## Common Vulnerabilities and Exposures

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

Bug ID	CVE references
511903	FortiAnalyzer 6.2.5 is no longer vulnerable to the following CVE-Reference(s): * CVE-2004-0230
610898	FortiAnalyzer 6.2.5 is no longer vulnerable to the following CVE-Reference(s): * CVE-2013-5211
597311	FortiAnalyzer 6.2.5 is no longer vulnerable to the following CVE-Reference: * CVE-2004-1653
606144	FortiAnalyzer 6.2.5 is no longer vulnerable to the following CVE-Reference: * CVE-2019-9193

# Known Issues

The following issues have been identified in FortiAnalyzer version 6.2.5. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

## Device Manager

Bug ID	Description
192706	After FortiAnalyzer added a VDOM, there is no method to disable VDOM mode.
545264	FortiAnalyzer may not show Device Lists.

## FortiView

Bug ID	Description
534761	FortiAnalyzer is missing threat entries in <i>FortiView &gt; Top Threats</i> .
542607	Drilldown <i>Applications &amp; Websites &gt; Top Web Sites(FortiClient)</i> always shows <i>No entry found</i> .
590775	FortiAnalyzer should hide <i>Device and Time Frame</i> selection in <i>FortiView Threat Map</i> .
611019	Filter is not working when drilling down from <i>Top Threats</i> .
612361	Compromised hosts do not show IP for <i>hostname resolution</i> .
621271	FortiAnalyzer may show incorrect session duration under <i>SOC &gt; Dial-up &gt; drill down table</i> .

## Log View

Bug ID	Description
559466	IOC drill-down may not show log data.
579871	Restoration of logs does not indicate correct timestamps under log browse after an NTP out of sync event.
596229	Log Filter should allow to choose and filter "DNS" log type when Log Forwarding is enabled.
597824	Base64 encoded filename within archived logs sent by FortiSandbox is not decoded on

Bug ID	Description
	FortiAnalyzer.
608139	Opening compressed FortiClient traffic file on FortiAnalyzer may cause other compressed FortiClient traffic logs fail to open.
640634	Logver field is not added to incoming logs resulting in empty charts.

## Others

Bug ID	Description
587489	Analytic data may be removed due to high disk usage.
601383	FortiAnalyzer may become unresponsive when source IPs change often for all endpoints due to DHCP.
602774	"execute backup logs" may trim the device list output if more than 4096 characters.
617669	File parser may keep crashing every few minutes.
635070	OFTP connection between the FortiGate unit and the FortiAnalyzer unit may fail to come up. This affects FGT_92D or lower. Workaround: On the FortiGate, disable reliable logging. To disable reliable logging, use the following commands in the CLI console: <pre>config log fortianalyzer setting   set reliable disable</pre>

## Reports

Bug ID	Description
547496	FortiAnalyzer generates a report for selected device with outputs for all devices.
553495	FortiAnalyzer may prompt <i>Web Server 404</i> Error when trying to download Report with 100,000 lines.
595715	Modified output profile may not take effect for Email generated report.
643238	User should be able to filter reports based on device name in <i>Reports &gt; Report Definitions &gt; All Reports</i> .

## System Settings

Bug ID	Description
593588	GUI should not allow creating a Local Certificate with <i>Certificate Name</i> containing more than 35 characters.
602422	Test User credentials fail when using <i>RADIUS MSCHAPv2</i> as authentication type.



# 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**<sup>®</sup>



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.